

IDA

INSTITUTE FOR DEFENSE ANALYSES

An Evolutionary Acquisition Strategy for the Global Command and Control Systems (GCCS)

Richard H. White, Project Manager
David R. Graham
Johnathan A. Wallis

DTIC QUALITY INSPECTED 2

September 1997

Approved for public release;
distribution unlimited.

IDA Paper P-3315

Log: H 97-001306

19980126 058

This work was conducted under contract DASW01 94 C 0054, Task T-J6-1492, for the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence). The publication of this IDA document does not indicate endorsement by the Department of Defense, nor should the contents be construed as reflecting the official position of that Agency.

© 1997, 1998 Institute for Defense Analyses, 1801 N. Beauregard Street, Alexandria, Virginia 22311-1772 • (703) 845-2000.

This material may be reproduced by or for the U.S. Government pursuant to the copyright license under the clause at DFARS 252.227-7013 (10/88).

INSTITUTE FOR DEFENSE ANALYSES

IDA Paper P-3315

**An Evolutionary Acquisition Strategy
for the Global Command and
Control Systems (GCCS)**

Richard H. White, Project Manager
David R. Graham
Johnathan A. Wallis

PREFACE

This paper is submitted by the Institute for Defense Analyses, under IDA task orders "C3 Systems Assessment," and "A Streamlined Acquisition Strategy for the Global Command and Control System (GCCS)." It formally documents the results of the deliberations of the GCCS Integrating, Integrated Product Team over the period November 1995 to November 1996 as they struggled to develop a business practice for future development and deployment of this new command and control system.

While the paper describes the end-to-end solution arrived at by all parties involved (J3, J6, the Services, DISA, ASD(C3I), DTSE&E, PA&E, and the Comptroller), it is not yet fully implemented as a business practice. The paper should therefore be regarded as the "model" approach to evolutionary acquisition for GCCS that is not yet a reality.

The authors wish to acknowledge reviewers Col. Mark Bennett, Mr. Ernest Brice, Ms. Angela Bruce, MAJ Richard Caldwell, Ms. Christine Condon, Capt. Cynthia DeCarlo, Mr. Douglas Fowler, Capt. Debbie Gross, Ms. Rosanne Hynes, Col. David Komar, Mr. Joe Krushinski, Col. Lawrence Machabee, Mr. Douglas McDonald, LTC Terry L. Mitchell, LTC David Quantock, COL William Reyers, Mr. John Saputo, LtCol David Searse, Mrs. Sandra B. Tewell, Mr. Paul Tavernier, Dr. Ronald Wilson, and Dr. Robert Anthony.

CONTENTS

PREFACE	iii
EXECUTIVE SUMMARY	ES-1
1. Global Command and Control System Evolutionary Acquisition Strategy: Introduction	1-1
A. What is Evolutionary Acquisition?	1-1
B. GCCS Evolutionary Acquisition Principles	1-2
1. Operating Premises	1-3
2. Burden Avoidance	1-3
3. Good Management	1-4
4. Integrated Product Teams	1-5
5. Continuous Business Process Reengineering	1-5
C. The Structure of This Strategy Paper	1-6
2. Mapping Evolutionary Acquisition Into DoD Regulation R-5000.2	2-1
A. 5000.2-R and GCCS Evolutionary Acquisition	2-1
B. The GCCS Evolutionary Acquisition Process	2-3
1. Evolutionary Acquisition Phases (EAPs)	2-4
2. Identifying and Incorporating Requirements Into the Acquisition Process	2-7
3. Requirements/Acquisition Oversight Process Compliance	2-11
3. Roles, Missions, and Integrated Product Teams	3-1
A. GCCS Stakeholders	3-1
B. Responsibilities and Lines of Authority	3-2
1. Office of Primary Responsibility	3-3
2. Joint Staff Responsibilities	3-3
3. Combatant and Functional Unified Commands	3-4
4. Military Services	3-5
5. Defense Information Systems Agency (DISA)	3-5

C. Acquisition Roles and Missions	3-5
1. Combining the Requirements and Acquisition Processes	3-6
2. Roles of Acquisition Oversight WIPTs	3-7
D. Security	3-15
E. Implementation Roles and Missions	3-17
1. Testing.....	3-17
2. Training.....	3-17
3. Contracting.....	3-17
4. Software and Hardware Support Services	3-17
5. Installation.....	3-18
6. Integrated Logistics Support (ILS).....	3-18
7. Transition Planning.....	3-18
4. Evolutionary Phase Implementation Plan (EPIP) Development.....	4-1
A. Scope of an EPIP.....	4-1
B. Contents of an EPIP Summary.....	4-2
1. Overview.....	4-2
2. Designation of Lead Performers	4-4
3. Evolutionary Requirements/Technical Solutions.....	4-4
4. Supporting Functions	4-5
5. Risk Overview	4-5
6. Testing.....	4-6
7. Economic Analysis and Cost as an Independent Variable	4-7
8. Evolutionary Phase Baseline (Cost, Schedule, Funding).....	4-9
C. EAP Finalization and Segment Roll-up.....	4-9
5. Conclusions and Recommendations	5-1
A. Formalizing Evolutionary Acquisition.....	5-1
B. Implement Improved Planning Process	5-2
C. Redefine Budgeting Approach.....	5-3
Glossary	G-1
Appendix A—Global Command and Control Management Structure.....	A-1
Appendix B—Global Command and Control System (GCCS) Functional Requirements Evaluation Procedures	B-1
Appendix C—GCCS Security Policy	C-1
Appendix D—v3.0 GCCS TEMP CONOPS	D-1

FIGURES

2-1	Overlay of GCCS Evolutionary Acquisition Strategy on DoD R-5000.2 Regulations	2-3
2-2	Milestones and Evolutionary Acquisition Phases	2-5
2-3	Evolutionary Acquisition Phases (EAPs) and Evolutionary Decision Reviews (EDRs)	2-6
2-4	EAPs, Segments, EDRs, and EPIPs	2-7
2-5	Unified Requirements/Acquisition Oversight Process	2-8
2-6	Requirements/Acquisition Oversight Process Compliance	2-11
3-1	GCCS Requirements and Operations Management Structure	3-4
3-2	GCCS Integrated Product Team Structure	3-6
3-3	United Requirements & Acquisition Oversight Process	3-7
3-4	Risk Assessment Process	3-9
3-5	Risk Assessment Considerations	3-10
3-6	Core, Related, and Contingent GCCS Economic Assessments	3-11
3-7	Illustration of Testing to Promote Risk Mitigation	3-13
4-1	Sample EPIP Table of Contents	4-3
4-2	Roll-up of GCCS Segments for an Evolutionary Acquisition Phase	4-11

EXECUTIVE SUMMARY

The Global Command and Control System (GCCS) is an intermediate step to establishing a joint Command, Control, Communications, Computing, and Intelligence (C4I) system of systems to provide total battle space information to the warrior. It is a distributed client-server-based architecture that incorporates a Common Operating Environment infrastructure with interfaces that support the hosting and execution of heterogeneous applications. This architecture has been designed, developed, and fielded not as a single system, but through periodic accretions of functionality and capability over the past three years.

This paper sets forth a streamlined, evolutionary acquisition strategy in support of continued rapid development and implementation of GCCS. This strategy is consistent with the DoD acquisition oversight framework. It tailors the DoD 5000.2-R regulation to apply those requirements needed to effectively manage the program.

DoD's customary approach calls for programs to specify in advance how all project funds will be allocated and spent—a “grand design” approach to acquiring weapons and systems within the budget cycle and, in the case of large systems, across many budget cycles. Unfortunately, within the current Program, Planning, and Budgeting System framework this means that the Department must project at least two or more years into the future to reserve the funding necessary to achieve objectives stated today. One alternative to planning total system design and resource demands at a single point in time has been termed “incremental” acquisition. This approach divides long-term projects into discrete increments (hence its name), each of which has clearly defined milestones and objectives. Evolutionary acquisition is an alternative to the grand design and incremental acquisition approaches. It is based upon the idea that *within a technologically dynamic environment, it is possible to pursue a long-term strategic vision by adopting a management and planning paradigm that, in the near term, allows development activities to quickly and flexibly respond to changing customer needs and technological opportunities.*

Successfully implementing evolutionary acquisition for GCCS begins by identifying desirable attributes for incorporation into the acquisition strategy. Based upon

the needs and representations of the GCCS community, three fundamental principles emerge: management flexibility, commonality across GCCS components, and continuity within and among CINCS. To be successful, GCCS evolutionary acquisition must avoid the tendency for new organizational paradigms to increase the complexity of oversight and management processes; to the extent practicable, the management of GCCS acquisition must be based upon existing organizational arrangements and procedures.

The development of strategies for, and oversight of, GCCS evolutionary acquisition is the responsibility of integrated product teams. Membership on these teams includes representatives from CINCs, Services, and Agencies (C/S/As), the Office of the Secretary of Defense, and other DoD organizations. Over time, through successive approximation and experimentation, and through collaboration on integrated product teams, the GCCS evolutionary acquisition strategy will itself evolve in an effort to continuously improve its functioning and responsiveness to warfighter needs. This is termed "continuous business process reengineering."

Within 5000.2-R, core activities are described in terms of acquisition phases and milestones. For the purposes of the GCCS evolutionary acquisition strategy, phases and milestones are interpreted within an evolutionary context. Milestones 0 and I are virtually identical to those described in 5000.2-R. Milestones II and III are significantly different however, because for evolutionary acquisition, the decisions to approve development and delivery/fielding are revisited each time additional capabilities or functionalities are planned. In particular, milestone approvals are replaced with Evolutionary Decision Reviews; the evolutionary aspects of the strategy begin after a Milestone II decision is made to proceed with the acquisition activity; and after the Milestone II decision is made to proceed with a new acquisition activity, GCCS enters an evolutionary phase cycle.

GCCS acquisition takes place according to Evolutionary Acquisition Phases, or EAPs. EAPs are discrete time periods during which resources are used to fulfill mission needs. They are described and structured according to a "contract" formulated and agreed to among all the members of the GCCS community. This contract, termed an Evolutionary Phase Implementation Plan, formalizes the objectives for GCCS during the EAP; sets forth cost, performance, schedule, test, economic, and budgetary issues; and identifies deliverable C2 capabilities.

To provide timely, flexible responses to warfighter needs, the GCCS evolutionary acquisition strategy integrates the requirements definition/validation/approval process with acquisition oversight to achieve early consideration of acquisition oversight

concerns. The result is a unified process which helps ensure the early, concurrent consideration of operational, technical, procedural, test, support, and fiscal issues within the GCCS stakeholder community. Within this process, the Chairman of the Joint Chiefs of Staff retains responsibility for policy guidance and oversight of global command and control; DOT&E, by law, has a separate line of authority, and by policy requires an operational test activity for GCCS. DOT&E has designated DISA/JITC as the OTA for GCCS.

The adoption of evolutionary acquisition principles by DoD in the area of information technology is particularly important due to the rapid advance of knowledge and know-how in the domain. It is vital that within such a technologically dynamic environment, long-term strategic visions be pursued by adopting a paradigm that in the near term allows development activities to quickly and flexibly respond to changing customer needs and technological opportunities. A management and planning framework that embraces such principles should be broadly applicable across not only C2 programs, but also within the larger Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) realm.

The following specific recommendations are intended to promote general application of evolutionary acquisition practices within the C⁴ISL community:

Recommendation: The ASD(C3I) should review, staff, and formalize the evolutionary acquisition principles developed for GCCS, and provide guidance as to their applicability for other C4ISR programs and activities within his/her purview. Deskbook input specific to automated information systems should be produced that interprets and tailors the DoD 5000 series of acquisition regulations for the C4ISR community. Such input should be submitted to the Defense Acquisition Policy Working Group for review.

Recommendation: The ASD(C3I) should staff an action to identify and select strategic planning tools that will support and comprise a strategic framework for management and planning within the C4ISR environment.. The staff should be directed to objectively consider extant tools residing in the government (military and civil) and in the commercial sector (domestic and foreign).

Recommendation: The ASD (C3I) should jointly staff an action with the Director, Program Analysis and Evaluation and the Comptroller to design a new accounting and budgeting methodology more suited to the rapid pace of change in technology and mission area realignment than currently possible within the extant PPBS process.

1. GLOBAL COMMAND AND CONTROL SYSTEM EVOLUTIONARY ACQUISITION STRATEGY: INTRODUCTION

The C4I for the warrior concept is committed to the challenge of meeting the warrior's quest for information needed to achieve victory for any mission, at any time and at any place. The C4I for the Warrior concept is the vision and a roadmap for providing such information support to the joint warfighter.

— General John M. Shalikashvili
Chairman of the Joints Chief of Staff

The Global Command and Control System (GCCS) is an intermediate step to establishing a joint Command, Control, Communications, Computing, and Intelligence (C4I) system of systems to provide total battle space information to the warrior. It is a distributed client-server-based architecture that incorporates a Common Operating Environment infrastructure with interfaces that support the hosting and execution of heterogeneous applications. This architecture has been designed, developed, and fielded not as a single system, but through periodic accretions of functionality and capability over the past three years.

This paper sets forth a streamlined, evolutionary acquisition strategy in support of continued rapid development and implementation of GCCS. This strategy is consistent with the DoD acquisition oversight framework. It tailors the DoD 5000.2-R regulation to apply those requirements needed to effectively manage the program.

A. WHAT IS EVOLUTIONARY ACQUISITION?

While the concept of acquiring weapons and systems for the Department of Defense on the basis of evolving requirements and technical solutions is not new, over the past 40 years continued demands for better oversight and accountability within both the Executive and Legislative branches of government have made employing such a strategy increasingly difficult. The key issue is how to assure those responsible for making national policy and securing the public interest that the public's monies are being well spent on meaningful and important projects. Three distinct approaches have been formulated and implemented to date.

DoD's customary approach calls for programs to specify in advance how all project funds will be allocated and spent—a "grand design" approach to acquiring weapons and systems within the budget cycle, and, in the case of large systems, across many budget cycles. Unfortunately, within the current Program, Planning, and Budgeting System (PPBS) framework this means that the Department must project at least two or more years into the future to reserve the funding necessary to achieve objectives stated today. In some cases, such as C4I, where a new generation of technology emerges as quickly as every 18 months, this means that DoD must anticipate what will be available one, two, or more generations into the future.

One alternative to planning total system design and resource demands at a single point in time has been termed "incremental" acquisition. This approach divides long-term projects into discrete increments (hence its name), each of which has clearly defined milestones and objectives. The intent of an incremental acquisition strategy is to allow large, long-term programs with well defined overall objectives to plan within shorter time horizons. It is especially suited to situations where the strategies and technologies to be applied in subsequent increments are strongly dependent upon the results of earlier increments. The increments themselves are rather rigidly defined, however, and not particularly well suited for cases where technological advance is fast paced.

Evolutionary acquisition is an alternative to the grand design and incremental acquisition approaches. It is based upon the idea that *within a technologically dynamic environment, it is possible to pursue a long-term strategic vision by adopting a management and planning paradigm that, in the near-term, allows development activities to quickly and flexibly respond to changing customer needs and technological opportunities*. It is particularly well suited when long-term goals are enunciated by senior DoD decision makers, but the specific path(s) to achieving those goals are not immediately known and are expected to be revealed as progress is made. Unlike incremental acquisition, evolutionary acquisition explicitly anticipates that successive achievements will be obsolesced by subsequent advances.

B. GCCS EVOLUTIONARY ACQUISITION PRINCIPLES

The strategy outlined in this paper is the result of a cooperative effort among the acquisition and technical communities over the period November 1995 to November 1996. During this period, representatives from all parts of the GCCS community participated in integrated product teams (IPTs, see Chapter 3) to identify evolutionary

acquisition principles and tailor them to the needs of command and control. Participants included representatives from ASD(C3I), PA&E, Comptroller, DOT&E, Joint Staff, DISA, and the Services. The following reflects a consensus opinion regarding the desirable traits for a successful evolutionary acquisition strategy for GCCS, and provides the guiding principles used to develop the strategy, as described in subsequent chapters.

1. Operating Premises

Successfully implementing evolutionary acquisition for GCCS begins by identifying desirable attributes for incorporation into the acquisition strategy. Based upon the needs and representations of the GCCS community, early on three fundamental principles emerged:

1. **Management Flexibility:** To ensure that GCCS is responsive to unmet warfighter needs in a timely manner, a distributed, flexible management philosophy must be practiced to maintain maximum freedom of action by decision makers at every level of management responsibility.
2. **Commonality Across GCCS Components:** A common operating environment (COE) must be established and must evolve in such a manner as to provide interoperability and ultimately integration of hardware and software systems at all component levels, according to warfighter needs.
3. **Continuity Within and Among CINCS:** GCCS must complement, without displacing, existing C2 capabilities within and among the CINCs, and must be implemented so as to harmonize with ongoing CINC C2 systems, plans, and strategies.

2. Burden Avoidance

To be successful, GCCS evolutionary acquisition must avoid the tendency for new organizational paradigms to increase the complexity of oversight and management processes. In keeping with the spirit of DoD acquisition reform initiatives, the GCCS community has expressed a firm desire to tailor a streamlined acquisition strategy that avoids:

- creation of new layers of bureaucracy;
- imposition of extra "wickets" to navigate, such as new regulations and rules;
- requirements for additional, unfunded resources (non-value-added activities);
- excessive interference with and burden on day-to-day operations.

- interference/delay of GCCS progress towards successive fielding of new functionalities.

3. Good Management

To the extent practicable, the management of GCCS acquisition shall be based upon existing organizational arrangements and procedures. In general, management should:

- **Use the existing, defined GCCS management structure laid out in CJCSI 6721.01.** This Instruction assigns the Joint Staff, J3 Operations Directorate, as the Office of Primary Responsibility. Roles and missions already assigned by this Chairman's Instruction will remain in effect and, where and when appropriate, will be modified by the Joint Staff. This management framework will serve as the foundation for the GCCS evolutionary acquisition strategy and the basis on which GCCS acquisition roles will be assigned.
- **Incorporate existing management and acquisition practices into the evolutionary acquisition framework.** All efforts will be made to avoid changes to existing working relationships and arrangements. Changes will be made only when they improve program outcomes. Measures of effectiveness for changes in management or for added oversight requirements include cost, performance, and schedule.
- **Retain current planning, implementation, and test and evaluation structures.** Ongoing practices for the management and planning activities for GCCS will be retained and modified to incorporate evolutionary principles. Test and evaluation will be conducted, commensurate with risk.
- **Use a flexible budgeting approach.** A modified level-of-effort funding cycle will be instituted to provide the budgeting flexibility necessary to cope with changing technological opportunities and warfighter needs. Budget preparation for the PPBS process will be based upon long-term strategic objectives and funds allocated to specific short-term tasks.
- **Clearly identify cost/schedule/thresholds.** GCCS will adopt a work "segment" planning process to identify and track cost, performance, and schedule for specific GCCS development tasks. Roll-ups of related segments will be used to create program baseline, test, economic analysis, and funding documentation.

4. Integrated Product Teams

The development of strategies for and oversight of GCCS evolutionary acquisition will be the responsibility of integrated product teams. Membership on these teams will include, as appropriate, representatives from DoD CINCs, Services, and Agencies (C/S/As), the Office of the Secretary of Defense, and other DoD organizations. In accordance with the *Rules of the Road*¹ for IPTs, GCCS evolutionary acquisition practices will employ these groups as a means for:

- coordinating objectives, schedules, and resources
- raising concerns and identifying mutually acceptable solutions
- adhering to IPPD/concurrency principles
- developing consensus on roles and responsibilities
- reviewing overall progress
- assuring that everyone's goals are met equitably and efficiently.

It is understood by the GCCS community that IPTs are not appropriate for:

- managing day-to-day operations
- promoting parochial goals or agendas
- deflecting responsibilities
- taking the place of ultimate management authority.

5. Continuous Business Process Reengineering

There is a need for flexibility in the development and deployment of new technologies to ensure that GCCS fields cutting-edge capabilities for the warfighter, and there is a need to continuously reexamine the means and mechanisms put in place for management and oversight. Over time, through successive approximation and experimentation, the GCCS evolutionary acquisition strategy will itself evolve in an effort to continuously improve its functioning and responsiveness to warfighter needs. This is termed "continuous business process reengineering."

¹ *Rules of the Road: A Guide for Leading Successful Integrated Product Teams*, (Department of Defense: Office of the Under Secretary of Defense for Acquisition and Technology), November 1995.

C. THE STRUCTURE OF THIS STRATEGY PAPER

The remaining chapters set forth the evolutionary acquisition strategy developed through the year-long process of the GCCS Integrating Integrated Product Team (IIPT). This strategy has been tested for the *Global Command and Control System (Top Secret)*, Phase 1, and is now being applied to Phase 2 of this effort as well as to version 3.0 of GCCS at the Secret level of classification.

- Chapter 2 provides an overview of the evolutionary acquisition strategy and describes how it conforms to the requirements of DoD 5000.2-R;
- Chapter 3 discusses the specific roles and missions of the different GCCS participating (stakeholding) organizations;
- Chapter 4 reviews the development of the key implementation document for GCCS evolutionary acquisition—the Evolutionary Phase Implementation Plan (EPIP);
- Chapter 5 concludes with a discussion of outstanding management issues, and recommendations for further action on formalizing evolutionary acquisition within the broader C4I environment.

The strategy draws on lessons learned from experience:

- there is a need for a common understanding among developers, requirements proponents, testers, financial managers, and users in the field;
- most activities reported under DoD 5000.2-R are value added when applied appropriately and tailored to specific programmatic characteristics;
- there is no major conflict between evolutionary acquisition objectives and means and the DoD 5000.2-R-R regulations.

We do find, however, that individual incentives of participants do not always support the broader objectives. Expediency discourages preparation of documentation, but this has inevitably caused problems downstream. Discipline is needed even for the streamlined approach discussed herein.

2. MAPPING EVOLUTIONARY ACQUISITION INTO DOD REGULATION 5000.2-R

The GCCS evolutionary acquisition strategy is fully consistent with DoD Regulation 5000.2-R, and represents an application of that regulation that is tailored to the unique needs of joint, global command and control. An evolutionary acquisition approach was chosen for GCCS for the following three reasons:

1. GCCS is an intermediate step to establishing a joint C4I system of systems to provide total battle space information to the warrior, a set of long-term goals enunciated by DoD senior leadership the attainment of which does not have a well defined trajectory.
2. Command and control opportunities, capabilities, limitations, and vulnerabilities are increasingly driven by commercial computing, telecommunications, and software market forces largely external to DoD.
3. The rate of introduction of new technologies is currently so rapid that no grand design or incremental approach can hope to adequately anticipate or take advantage of unforeseen and emerging opportunities.

A. 5000.2-R AND GCCS EVOLUTIONARY ACQUISITION

GCCS does not fit the traditional mold of an acquisition program and is better described as an "acquisition activity." It has all of the characteristics of a program, but due to its broad, overarching goals and impacts across Defense Agencies and Services, the notion of a unified program is not particularly meaningful in the GCCS context. For the purposes of 5000.2-R, GCCS is characterized as an ACAT IAM¹ acquisition activity

¹ "ACAT IA programs are MAISs [Major Automated Information Systems]. A MAIS is estimated by the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)) to require program costs for any single year in excess of \$30 million (FY 1996 constant dollars), total program costs in excess of \$120 million (FY 1996 constant dollars), or total life-cycle costs in excess of \$360 million (FY 1996 constant dollars), or those designated by the ASD(C3I) to be ACAT IA. . . . An "ACAT IAM [program is one] for which the MDA [Milestone Decision Authority] is the Office of the Secretary of Defense (OSD) Chief Information Officer (CIO) (formerly the Senior IM Official, the ASD(C3I)). The "M" refers to Major Automated Information Systems Review Council (MAISRC)." DOD 5000.2-R, ¶1.3.2.

“for which the MDA [Milestone Decision Authority] is the Office of the Secretary of Defense (OSD) Chief Information Officer (CIO).”²

The evolutionary acquisition strategy employed by GCCS is fully compliant with 5000.2-R and tailored to provide the planning and implementation flexibility necessary to allow joint C2 capabilities to keep pace with changing requirements and technological opportunities. According to 5000.2-R, all DoD ACAT IAM acquisition activities shall “accomplish certain core activities” which shall be “tailored to minimize the time it takes to satisfy an identified need consistent with common sense and sound business practice.”³ The strategy addresses these core activities by including processes for requirements identification, validation, priority setting, technical and economic evaluation, risk assessment, development and operational testing, and acquisition oversight and management.

Within 5000.2-R, core activities are described in terms of acquisition phases and milestones. For the purposes of the GCCS evolutionary acquisition strategy, phases and milestones are interpreted within an evolutionary context. Milestones 0 and I are virtually identical to those described in 5000.2-R. Milestones II and III are significantly different, however, because, for evolutionary acquisition, the decisions to approve development and delivery/fielding are revisited each time additional capabilities or functionalities are planned. Figure 2-1 overlays the GCCS strategy on the 5000.2-R process.

Note the following differences from a more traditional grand design or incremental acquisition approach.

- Milestone approvals are replaced with Evolutionary Decision Reviews (EDRs). For each EDR, the ASD(C3I) and/or his/her designee, at his/her discretion, may choose to convene a formal meeting of the MAISRC [Major Automated Information System Review Council] or conduct the MAISRC through other means including, but not limited to, paper, electronic (e.g. email), and video tele-conference (VTC). This is particularly expeditious because it allows decisions to be delegated according to the level of risk.
- The early EDRs corresponding to Milestones 0 and I, and I and II, still focus on concept development and early stage planning activities to determine whether a new acquisition activity should be approved. The evolutionary aspects of the strategy, therefore, really begin after a Milestone II decision is made to proceed with the acquisition activity.

² DOD 5000.2-R, ¶1.3.2.

³ DOD 5000.2-R, ¶1.4.

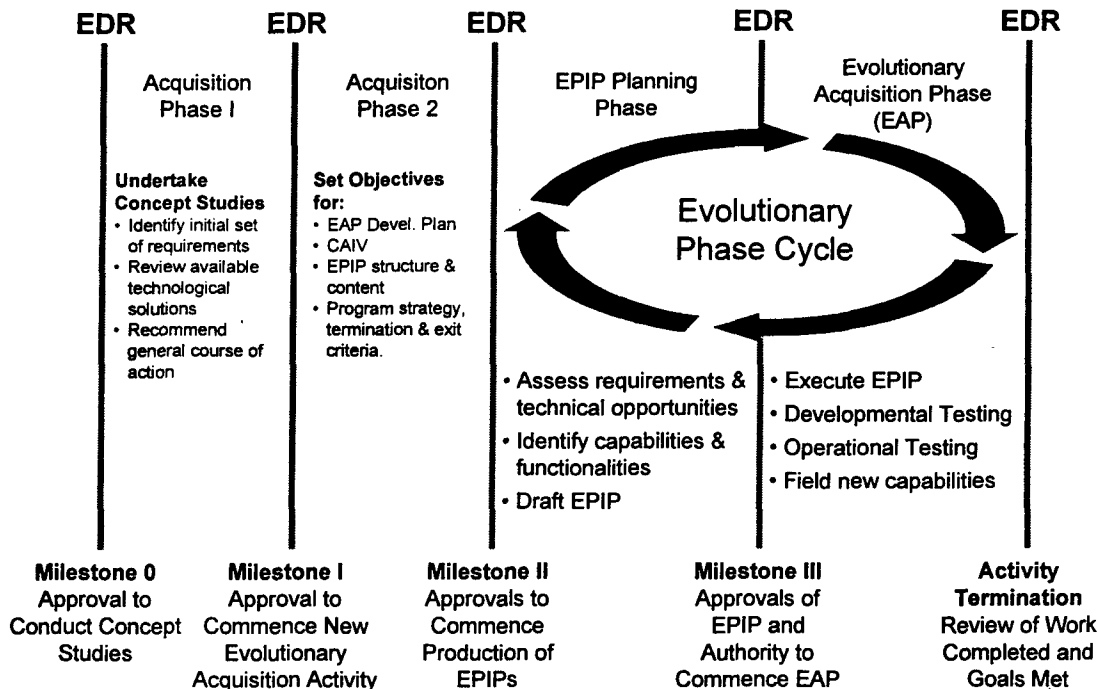


Figure 2-1. Overlay of GCCS Evolutionary Acquisition Strategy on DoD 5000.2-R Regulations

- After the Milestone II decision is made to proceed with a new acquisition activity, GCCS enters an evolutionary phase cycle. This cycle comprises two successive parts. The first is an Evolutionary Phase Implementation Plan (EPIP) planning phase; the second is the Evolutionary Acquisition Phase (EAP) (see below). Evolutionary acquisition activities proceed according to this cycle, punctuated by periodic EDRs to approve requirements, plans, and implementation activities.

B. THE GCCS EVOLUTIONARY ACQUISITION PROCESS

This section provides an overview of the decision making and documentation processes embodied in the GCCS evolutionary acquisition strategy. Its purpose is to offer a framework for working concepts and a road map of the functioning of the strategy that will be elaborated in subsequent chapters. In accordance with 5000.2-R, it addresses how the process is designed to ensure that performance objectives and minimum acceptable requirements for GCCS will remain consistent with the statement of operational capability need set forth in the May 1995 *Mission Need Statement (MNS) for Global*

*Command and Control System.*⁴ The GCCS evolutionary acquisition strategy employs a variety of new terms to describe the activities and procedures incorporated to afford flexible and responsive oversight.

1. Evolutionary Acquisition Phases (EAPs)

The GCCS evolutionary acquisition strategy is grounded in two basic concepts. The first is that all aspects of acquisition--the conception, design, development, implementation, testing, fielding, and delivery, of C2 systems--should be highly responsive to the needs of the customer, in this case the warfighter. The second is that C2 system development cycles must be short enough to take timely advantage of emerging technologies. To meet these two goals, GCCS acquisition takes place according to Evolutionary Acquisition Phases, or EAPs.

EAPs are discrete time periods during which resources are used to fulfill mission needs. They are described and structured according to a "contract" formulated and agreed to among all the members of the GCCS community. This contract, termed an Evolutionary Phase Implementation Plan (EPIP), formalizes the objectives for GCCS during the EAP, sets forth cost, performance, schedule, test, economic, and budgetary issues, and identifies deliverable C2 capabilities. This contract:

1. meets the requirements set forth in 5000.2-R, and
2. coordinates activities of diverse players.

While less rigid than the traditional Milestone process, the evolutionary strategy is structured enough to ensure proper management, and that appropriate programmatic issues are raised, communicated, and resolved.

In terms of Figure 2-1, both EPIP planning and execution for successive EAPs take place concurrently, so Evolutionary Decision Reviews (EDRs) for overlapping Milestone II and III decisions are collapsed into a single oversight decision. Redrawing Figure 2-1 to conform with this notion results in Figure 2-2. It shows that both planning and execution occur on a continuous basis, punctuated by EDRs. Planning and preparation for subsequent EAPs occurs during execution of the current EAP. The strategy therefore implements a so-called "rolling" approach to planning where

⁴ Department of Defense, (May 1995), *Mission Need Statement (MNS) for Global Command and Control System (GCCS)*.

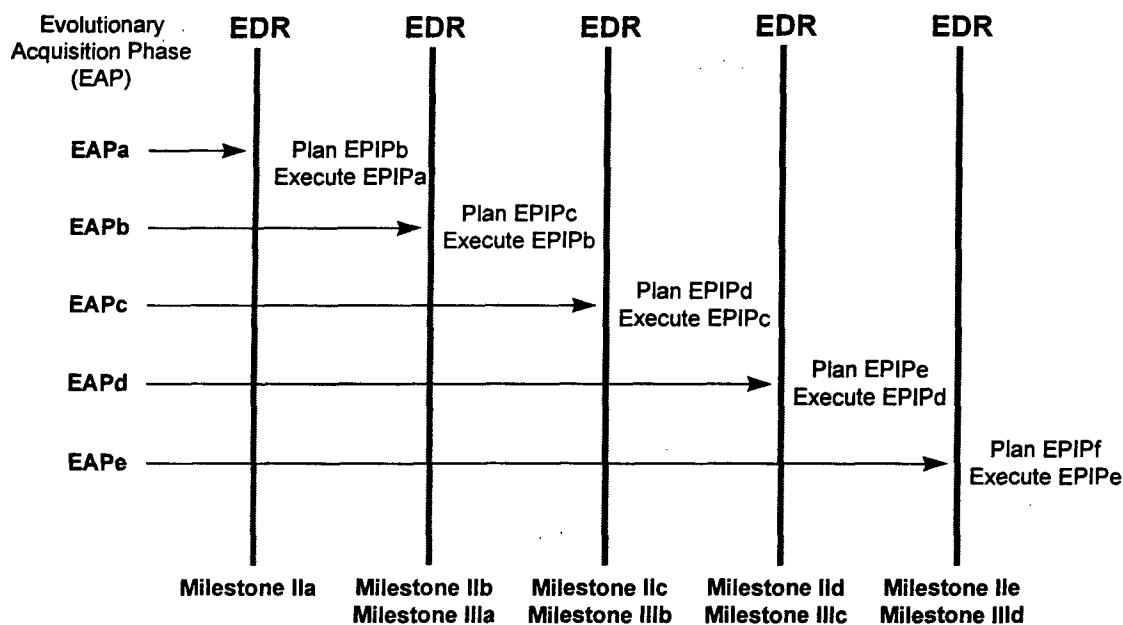


Figure 2-2. Milestones and Evolutionary Acquisition Phases

successive baselines are developed and revised according to requirements, development, deployment, and fielding schedules.

Based upon the needs of the warfighter, technological opportunities, and resources available, an EDR is scheduled to assess ongoing EAP progress and at the same time approve the implementation of new EIPs, as shown in Figure 2-3. Unlike traditional milestone reviews, EDRs are conducted at the lowest possible level of approval authority commensurate with the risk inherent in the proposed EIP and based upon the success of ongoing development and management activities. EDRs need not, and in general do not, involve the convening of a MAISRC. Rather, the responsibility for decision making lies with empowered subordinates of MAISRC members.

Figure 2-3 traces the basic evolutionary acquisition process from requirements through fielding. In the upper left-hand corner, it begins with the users who identify and validate requirements. This leads to proposed technical solutions from the performer (developer) community and evaluation measures proposed by the testers. The confluence of requirements, measures of performance, and proposed technical solutions leads to a negotiation between the users, testers, and performers, the results of which are captured in the EIP. As the contract between users, testers, and performers, the EIP identifies what will be fielded when, and how technical solutions will be implemented. As such, the

architecture, configuration, costs, funding, schedules, test regimes, and performance expectations are all contained within the EPIP. Once the EPIP is finalized among the

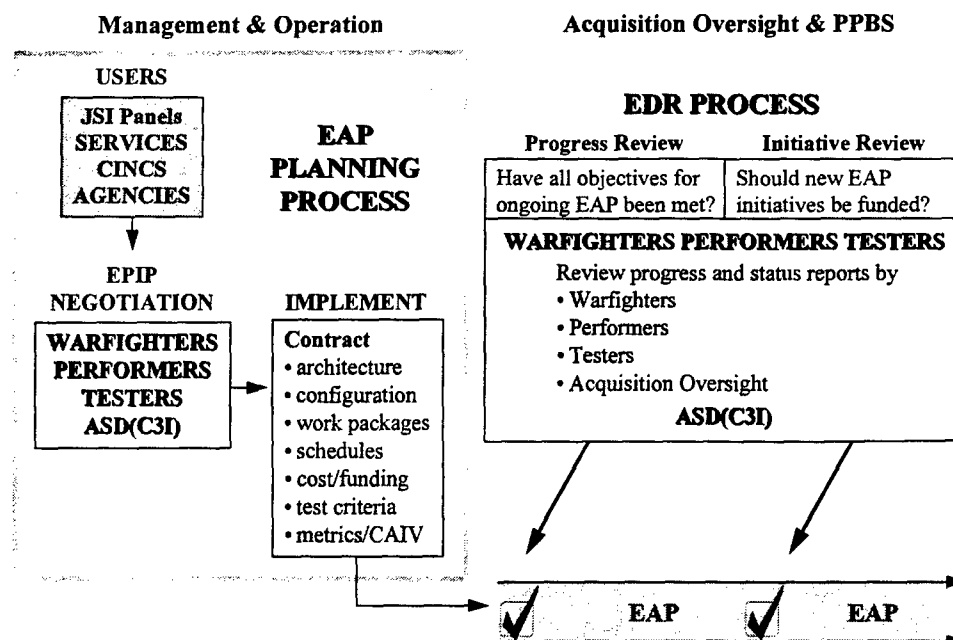


Figure 2-3. Evolutionary Acquisition Phases (EAPs) and Evolutionary Decision Reviews (EDRs)

user, tester, and performer, it is submitted for review by the oversight community. An EDR is then held. This may be a paper process involving only formal coordination, or could be the result of a video teleconference or face-to-face meeting of principals. Approval of the EPIP via the EDR signals formal permission for the performer to begin development activities (commencement of the EAP) and to continue through to fielding.

For planning and execution purposes, the work done during an EAP is divided into manageable and responsive Segments. Each Segment comprises a distinct development effort assigned to one or more GCCS stakeholder organizations, and a set of deliverables (see Figure 2-4). Segments provide a logical means for progressively translating broadly stated mission needs into well defined system-specific tasks and ultimately into operationally effective, and suitable systems.

GCCS evolutionary acquisition is a sequence of EAPs. To provide flexibility, Segments defined and begun during one EAP may continue beyond the end of that EAP, and in some cases might span more than two EAPs. When this occurs, Segment progress is reviewed during EDRs and a decision to continue, modify, or discontinue the Segment

is made at that time. In this way the GCCS community may plan long-term activities and adjust project "trajectory" over time to comport with new technological opportunities and

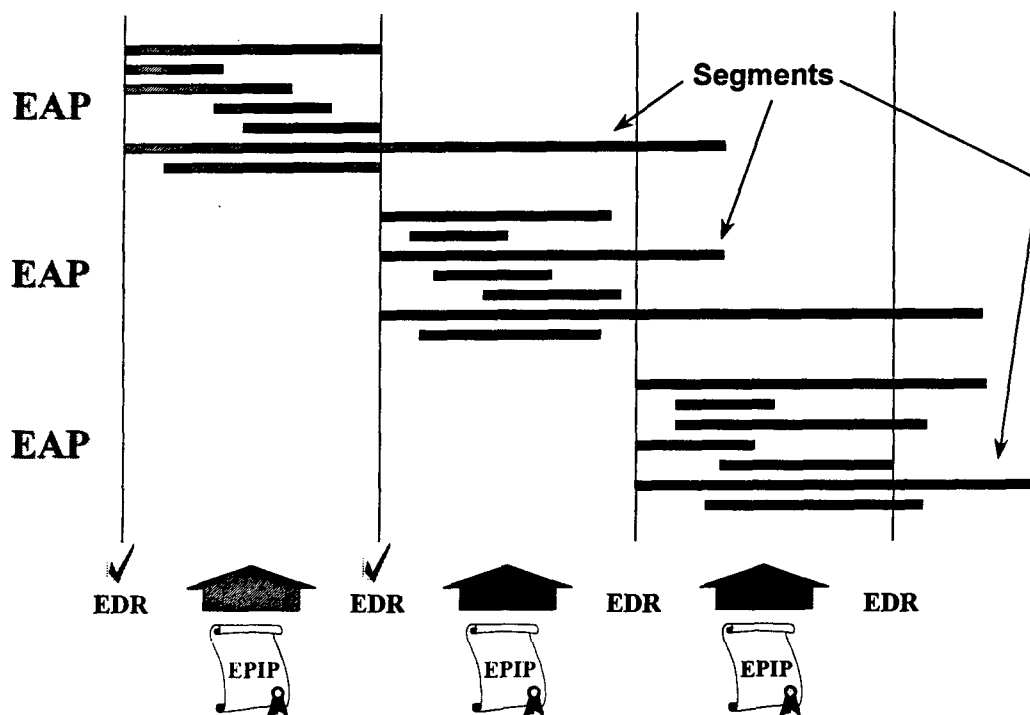


Figure 2-4. EAPs, Segments, EDRs, and EPIPs

changing requirements. In addition, this structure allows rapid shifts in direction, and corresponding changes in resource allocation to warfighter needs *within* the Program Objectives Memorandum (POM) cycle.

2. Identifying and Incorporating Requirements Into the Acquisition Process

To provide timely, flexible responses to warfighter needs, the GCCS evolutionary acquisition strategy integrates the requirements definition/validation/approval process with acquisition oversight to achieve early consideration of acquisition oversight concerns. The result is a unified process which helps ensure the early, concurrent consideration of operational, technical, procedural, test, support, and fiscal issues within the GCCS stakeholder community. As shown in Figure 2-5, the unified process has six formal steps leading up to the decision to field: 1) Identify Requirements, 2) Validate Requirements, 3) Assessment I, 4) Prioritize Requirements, 5) Assessment II, and 6) Develop.

Figure 2-5 also depicts the relationship between the requirements and acquisition oversight processes (including development and fielding), and the interaction between the

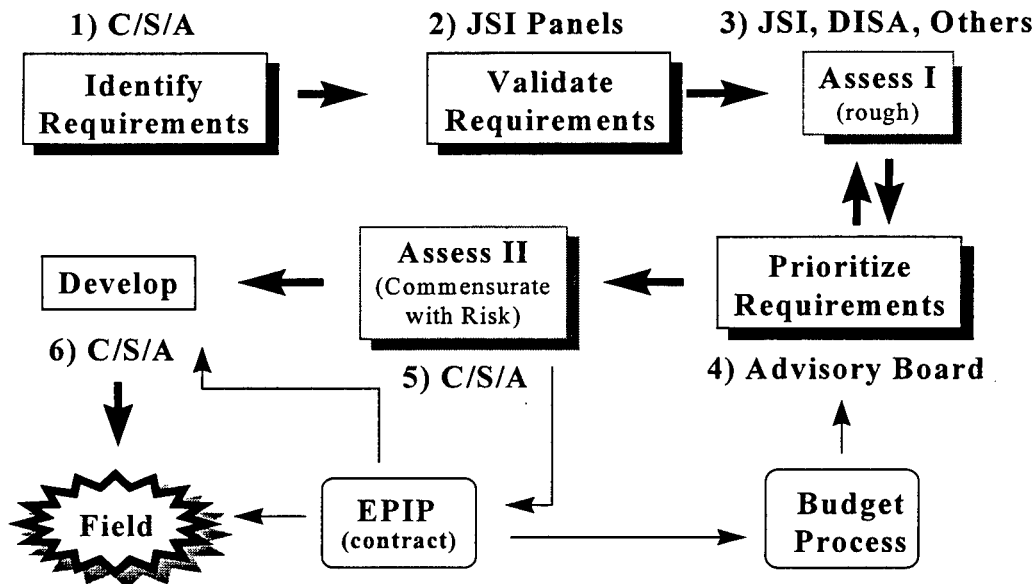


Figure 2-5. Unified Requirements/Acquisition Oversight Process

requirements process and the acquisition/development process. Black-bordered boxes are activities led by the Joint Staff; gray-bordered boxes are activities led by the acquisition oversight community.) It illustrates a sequential process from identification of a requirement to fielding of a capability to meet that requirement. In reality, this process is iterative, and continuous “feedback” between different steps is anticipated and encouraged.

a. Steps 1 & 2: Identify and Validate Requirements

The Joint Staff, J3, has the responsibility for identifying and validating GCCS requirements. This is formally laid out in Chairman of the Joint Chiefs of Staff Manual, CJCSM 6721.01 (Appendix B), and the process is fully compliant with 5000.2-R. The J3 solicits requirements from CINCs, Services, and Agencies (C/S/As), and receives and catalogs unsolicited requirements on an ongoing basis [Step 1]. Requirements may come from Advanced Technology Demonstrations (ATDs), Joint Warfighting Interoperability Demonstrations (JWIDs), special studies, and other sources. A comprehensive database, the GCCS Requirements Database (GRiD), has been established by J3 to catalog and retain all requirements submitted and record their disposition in the review and assessment process.

According to the GCCS management procedures established under CJCSI 6721.01 (Appendix A), all requirements collected are passed to review panels (JSI Panels) comprised of representatives from DoD C/S/As. Requirements are reviewed for validity, including a determination of whether or not a requirement is joint and therefore properly assigned to GCCS, a duplicate of other requirements submitted, or a subset of existing, planned, or submitted requirements [Step 2].

b. Step 3: Assessment I

Given a validated requirement, Assessment I (Assess I) provides an initial, rough estimate of what is needed for technical implementation, including an appreciation of associated risks. To the extent possible, it affords a basis for consistently assigning priorities to requirements. The intended result is a balanced picture of candidate solutions and prudent hedges against risks to ensure that easily ascertainable attributes have been identified and considered. Obvious threats to successful implementation of potential technical and operational solutions are recorded for use in later, more in-depth assessments (see Step 5: Assessment II, below).

As part of Assess I, generic frameworks may be employed to provide a check on the logical completeness of candidate technical and operational solutions. These would generally include characterization of:

- **Mission criticality** to focus the assessment on the consequences of failing to meet the requirement, such as degradation of operations, to levels much below planned operational baselines. Testers assist users to articulate mission criticality and avenues for risk mitigation.
- **Requirements and their logical consistency** to highlight inherent contradictions and identify mission-level tradeoffs facing developers and commanders.
- **Candidate technical and operational solutions** developed by users and developers to examine technical/operational trade-offs necessary to implement a solution affordably.
- **Estimates of cost, performance, and schedule** to provide decision makers with additional information necessary to comply with cost as an independent variable (CAIV) considerations.

The output of Assess I is a decision memorandum for the GCCS Review Board which provides a strawman ranking of requirements in priority order.

c. Step 4: Review Board Prioritization

A Review Board composed of representatives from the C/S/As and chaired by the Vice J6 is charged with the task of assigning final priorities to requirements. Based upon the results of Assess I, the Board makes trade-offs among mission need, technical maturity, anticipated benefits, perceived risks, and resource demands associated with proposed technical solutions. The output of the Review Board is a recommendation to the General Officer/Flag Officer (GO/FO) Board regarding technical solutions to be implemented and a rough estimate of schedule. The set of requirements approved for implementation by the GO/FO Board becomes the basis for an EPIP.

d. Step 5: Assessment II and EIPs

The development of an EPIP is addressed in detail in Chapter 4. The activity that takes place to develop the plans and information necessary to formalize an EPIP is Assessment II (Assess II). Based upon the requirements approved for implementation by the GO/FO Board, the GCCS stakeholders collaboratively work to scope the technical details, cost, performance, test, budget, schedule, security, operations, maintenance, and resource allocations necessary to undertake development activities and field a new capability. In effect, Assess II is a more formally structured and more in-depth treatment of issues addressed in Assess I.

It is important to understand and emphasize that evolutionary acquisition is intended to be a "mass customization" process where the intensity (depth) of assessments is commensurate with the anticipated level of risk associated with fielding a new capability. While Assess II is therefore more detailed than Assess I, it is not a "one size fits all" activity.

e. Step 6: Development

Once an EPIP has been written, concurred with, and signed out by the decision authority, technical development begins. Because the process is evolutionary, there may be considerable overlap between development and fielding, as segments mature and are deployed to users. In the case of GCCS, the decision authority is a jointly held responsibility by the Director of Operations, J3, Joint Staff, and the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence. In the case of a new core system, a TEMP must be developed and separately coordinated with users,

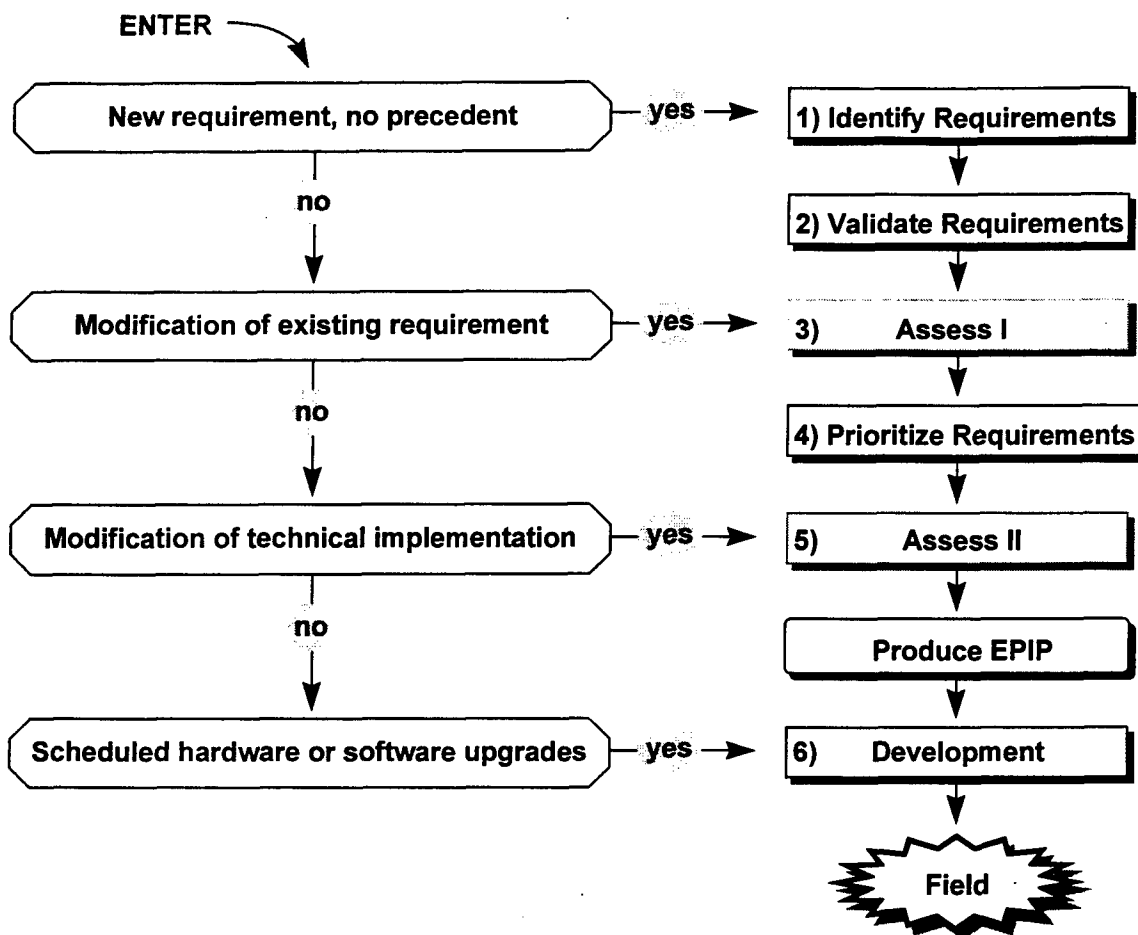


Figure 2-6. Requirements/Acquisition Oversight Process Compliance

developers, and testers, and approved by DTSE&E and DOT&E.) Acquisition oversight activities continue during this step, including testing and fielding.

3. Requirements/Acquisition Oversight Process Compliance

The six-step unified requirements/acquisition oversight process just discussed is more flexible than it appears from Figure 2-5. In many cases, requirements are already known and/or prioritized and will enter the process at a later step. Depending on the nature of the GCCS requirement or technical solution, again the “no one size fits all” rule applies. In some cases, the requirements placed on the system may also come from outside the GCCS requirements process. This may be as a result of unique Service or CINC needs that must be integral to the deployment of the system. As shown in Figure 2-6, if a brand new requirement is being proposed, it will go through the entire process. If

the proposed action is a change to an existing requirement, such as expanding JOPES to handle Reserve data as expressed by the Commission on Roles and Missions, this requirement will enter at the first assessment process [Step 3]. Modifications to the technical implementation of an existing capability will be assessed as part of a proposed GCCS phase or package and enter directly into an Assess II activity [Step 5]. This includes fundamental or widespread technical modifications that entail significant transition risks and/or changes to support procedures. Finally, scheduled upgrades to hardware or software will be handled as part of GCCS configuration management and proceed directly to development [step 6].

For instance, for GCCS(T), requirements and technical solutions already existed and the replacement of WWMCCS at the Top Secret level was implemented in a manner closely following that of the Secret system. As such, the process began at the "modification of technical implementation," Step 5. For GCCS (3.0) stage 1, the introduction of a new operating system and database management system carries significant risk due to technical incompatibilities with GCCS (2.2). It was therefore treated as an Assess II, Step 5 modification requiring an EPIP and extensive testing. For GCCS (3.0), stage 2, the introduction of new requirements was handled by the Joint Staff requirements Panels set up by CJCSI 6721.01, and Requirements Implementation Documents (RIDS) were developed. These RIDs intersected the ongoing plans to improve and up-grade GCCS from version 2.2 to version 3.0. No Assess I was undertaken because the capabilities to be provided were already available and operational as a result of prior development and testing activities. For this reason, the formal evolutionary acquisition process again commenced at Step 5, the "modification of technical implementation."

3. ROLES, MISSIONS, AND INTEGRATED PRODUCT TEAMS

The National Command Authorities (NCA) implement command and control through a process that extends global influence over our national agencies, military forces, allies, and ultimately, over our adversaries. The process functions through a system which provides NCA and subordinate leaders with a means to exercise their authority and direction; it uses information to coordinate resources toward common mission objectives; and it involves a continuous dynamic interaction between information, the organization, and a support system for warfighting CINCs, subunified commands, CJTFs, their respective Service components, and coalition forces.¹ This dynamic interaction requires a responsive and flexible approach to acquisition management.

This chapter discusses how the respective roles and missions of all organizations involved in the conception, design, development, implementation, evolution, and life-cycle maintenance of GCCS relate to OSD oversight functions. In particular, it explains how the various organizations come together in deliberative planning fora, termed integrated product teams (IPTs), as called for in DoD's *Rules of the Road: A Guide for Leading Successful Integrated Product Teams*.² Henceforth, organizations so involved are termed "GCCS stakeholders," or "stakeholders."

A. GCCS STAKEHOLDERS

There are three logical groupings or communities of GCCS stakeholders: users, performers, and acquisition oversight. The following organizations are GCCS stakeholders for whom acquisition roles and missions are defined and who are formally represented on IPTs.

¹ Department of Defense, (May 1995), *Mission Need Statement (MNS) for Global Command and Control System (GCCS)*.

² Department of Defense, (November 1995), *Rules of the Road: A Guide for Leading Successful Integrated Product Teams*.

Users

Joint Staff

- Director for Intelligence, J2
- Director for Operations, J3
- Director for Command, Control, Communication, and Computer Systems, J6

Services

- Army
- Navy
- Air Force
- Marines
- ASD (C3I) DASD (C3), as the cognizant PSA

Performers

Defense Information Systems Agency (DISA)

Defense Special Weapons Agency (DSWA)

Services

Acquisition Oversight

Office of the Assistant Secretary of Defense, Command, Control, Communication, and Intelligence (C3I), DASD (C3I Acquisition)

Program Analysis and Evaluation (PA&E)

ODOT&E

ODTSE&E/T&E

Joint Interoperability Test Command (JITC)

Service Operational Test Activities

Office of the Comptroller

B. RESPONSIBILITIES AND LINES OF AUTHORITY

The Chairman of the Joint Chiefs of Staff is responsible for policy guidance and oversight of global command and control, and this is transmitted to the Director of the Joint Staff for implementation. Joint Staff authority for GCCS management and implementation devolves from the Chairman as set forth in CJCSI 6721.01, dated 18 February 1995, and is incorporated by reference in this Strategy. Appendix A includes

the full text of CJCS 6721.01, which establishes a formal management structure.³ In addition to the Joint Staff, DOT&E, by law, has a separate line of authority, and by policy requires an operational test activity for GCCS. DOT&E has designated DISA/JITC as the OTA for GCCS.

1. Office of Primary Responsibility

The Director for Operations, J3, Joint Staff, is the Office of Primary Responsibility (OPR) for GCCS. Responsibilities include:

- planning and Program Budget System Submissions for funds managed by the Joint Staff and DISA;
- approval for development and implementation of processes and capabilities that support GCCS;
- direction of revisions to current planning and execution procedures to match current national strategy and the Unified Command Plan (UCP); and,
- chairmanship of the GCC Flag Officer/General Officer Advisory Board.

As described in detail in CJCSI 6721.01 and depicted in Figure 3-1, the OPR, J-3, is assisted by:

- the GCC General Officer/Flag Office Advisory Board,
- the GCC Review Board, and
- The GCC Functional Area and C4 Systems Integration Working Groups (JSI Panels).

2. Joint Staff Responsibilities

The GCCS responsibilities of other Joint Staff Directorates are as follows:

- **Director for Manpower and Personnel, J1.** Assists the OPR by exercising responsibility for all GCC issues relating to personnel support systems.
- **Director for Intelligence, J2.** Assists the OPR by exercising oversight of intelligence systems development, integration, and management of intelligence automated information activities in GCCS, including integration of non-DoD intelligence community systems.
- **Director for Logistics, J4.** Assists the OPR by exercising responsibility for mobilization, demobilization, sustainment, reconstitution, deployment, and redeployment policy and procedure definition, and for management of related prototype development efforts.

³ A complete description of these responsibilities and authorities is contained in Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6721.01 (18 February 1995).

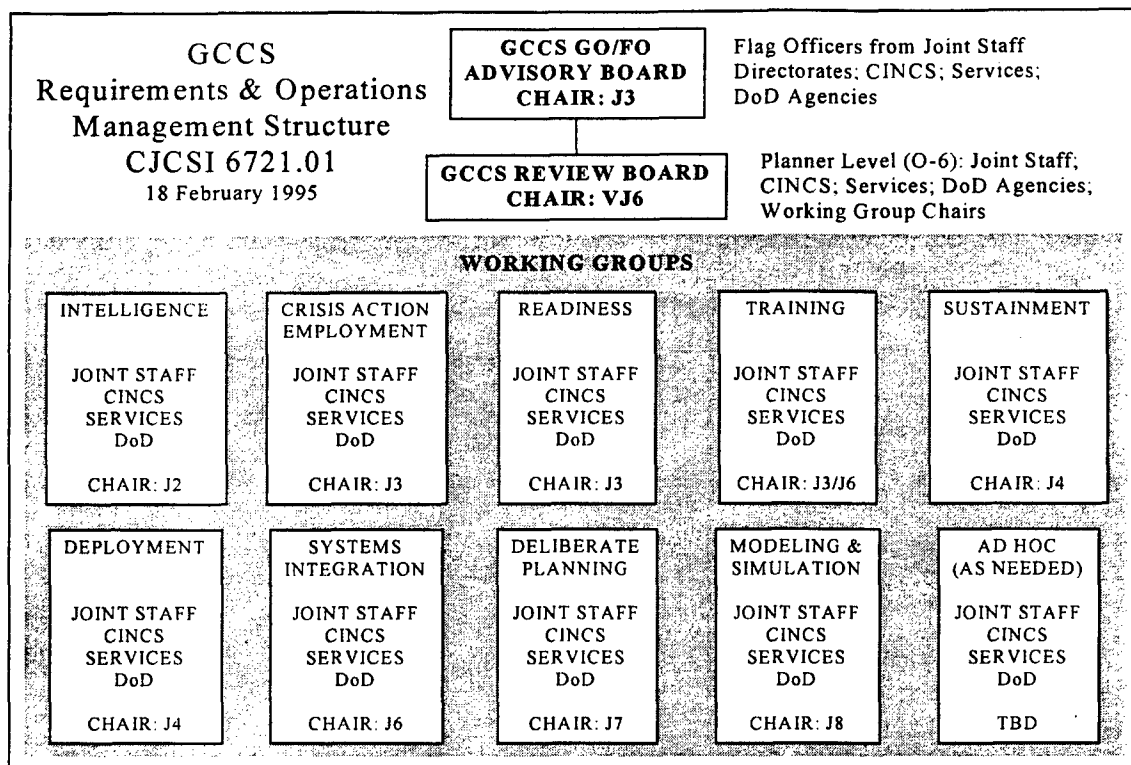


Figure 3-1. GCCS Requirements and Operations Management Structure

- **Director for Strategic Plans and Policy, J-5.** Serves as the Joint Staff point of contact for GCCS coordination with non-DOD agencies.
- **Director for Command, Control, Communications, and Computer Systems, J-6.** Assists OPR by serving as system implementer and executing technical oversight for all C4 system development, ADP integration, and management of technical activities in GCCS, operation and maintenance of the network, data administration, and communications management.
- **Director for Operational Plans and Interoperability, J-7.** Assists the OPR by executing responsibility for development, integration, and documentation of GCCS procedures, and reviews planning.
- **Director for Force Structure, Resources, and Assessment, J-8.** Coordinates with OPR to determine GCCS effects on and potential interactions with modeling and simulation, and advises OPR on such matters.

3. Combatant and Functional Unified Commands

The GCCS responsibilities for combatant and functional unified commands are to:

- Provide flag-level representatives to the GCC General Officer/Flag Officer Advisory Board.

- Provide O-6 representatives to the GCC Review Board.
- Participate in other GCCS working groups as required, including the provision of requirements, facilitation of test beds, oversight system maintenance, and establishment of ad hoc working groups to ensure information is made available throughout commands.

4. Military Services

The GCCS responsibilities for the military Services are to:

- Provide flag-level representatives to the GCC General Officer/Flag Officer Advisory Board.
- Provide O-6 representatives to the GCC Review Board.
- Provide representatives to Functional Area and C4 Systems Integration Working Groups.
- Provide planning, coordination, PPBS, operations, maintenance, and information support as required.

5. Defense Information Systems Agency (DISA)

The GCCS responsibilities for DISA are to:

- Serve as executive agent of the Joint Staff for GCCS and for the transition efforts that migrate current systems to GCCS.
- Provide the Project Manager for GCCS, who in turn provides oversight and direction of activities in DISA, including integration, testing, and fielding of all GCCS ADP applications in accordance with Joint Staff guidance.
- Manage the long-haul communications network that supports GCCS connectivity to each site's GCCS premise router, and technical assistance for local connectivity requirements.

C. ACQUISITION ROLES AND MISSIONS

The GCCS evolutionary acquisition strategy builds upon the roles and missions of organizations formally involved with GCCS as set forth in CJCSI 6721.01.⁴ Members of each GCCS stakeholder community have multiple roles to play in the acquisition process, and serve on a variety of boards, panels, and teams. Figure 3-2 illustrates the organization and membership of top-level GCCS acquisition organizations.

⁴ Appendix A reproduces CJCSI 6721.01 in its entirety.

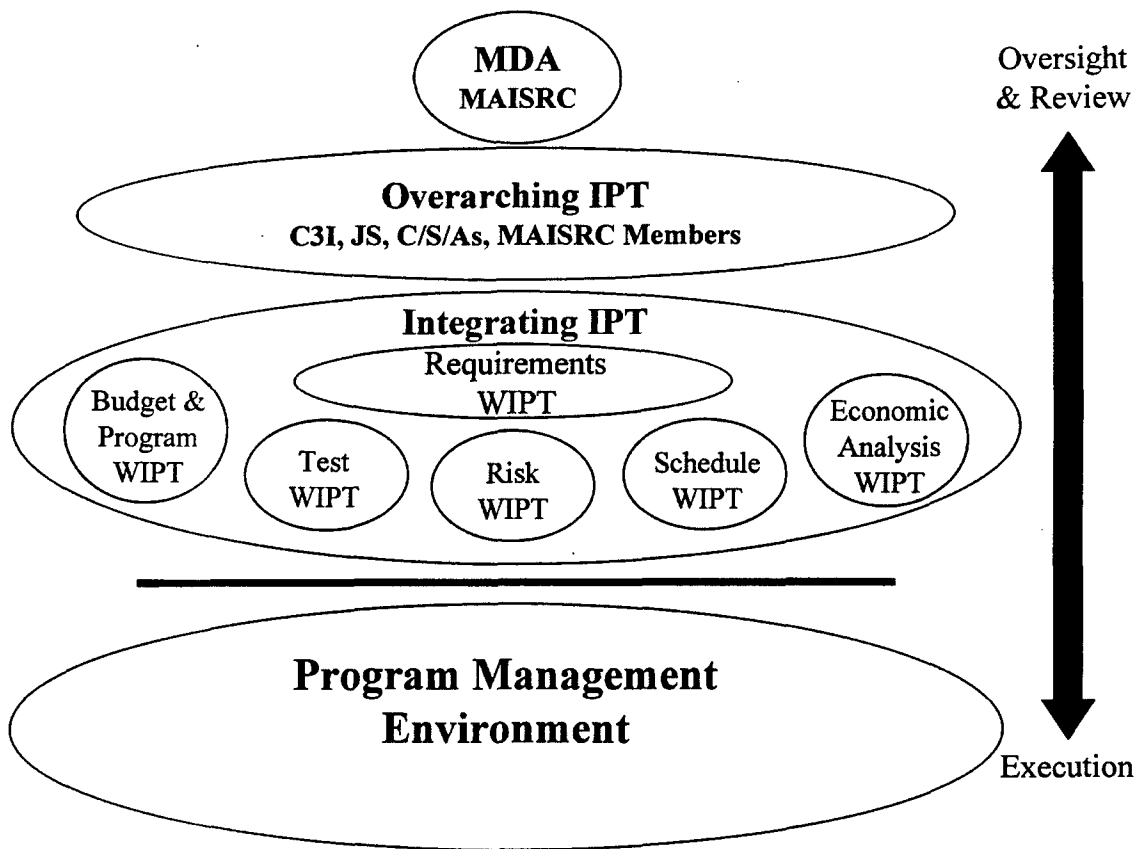


Figure 3-2. GCCS Integrated Product Team Structure

Note that, as called for in *Rules of the Road*, there are two IPT levels below the milestone decision authority: overarching and working-level. The working-level IPTs (WIPTs) are assigned specific functions related to acquisition activity oversight, management, and budgeting, and collectively form the Integrating IPT (IIPT). In addition, WIPTs (JSI Panels) dealing with requirements that are within the purview of the Joint Staff are also considered to be part of the IIPT. Membership on the various IPTs is open and unrestricted. At a minimum, each IPT must contain representatives from organizations key to decision making in their respective areas of responsibility.

1. Combining the Requirements and Acquisition Processes

As discussed, for joint C2 the Chairman's Instruction CJCSI 6721.01 establishes an advisory General Officer/Flag Officer Board and a requirements Review Board, and appoints the Joint Staff Directorate for Operations (J-3) as the Office of Primary Responsibility (OPR) for joint C2. Advice to the OPR is provided through the GO/FO Board, which meets on an ad hoc basis, as needed; requirements identification and

validation are overseen by the Review Board; and JSI Panels are used to address intelligence, crisis action employment, readiness, training, sustainment, deployment, systems integration, deliberate planning, modeling and simulation, and other issues. Specific details regarding the functioning of the GCCS requirements identification and validation process are contained in CJCSM 6721.01 (see Appendix B).

The requirements process forms the basis for the GCCS evolutionary acquisition strategy, as discussed in Chapter 2. WIPTs necessary to carry out acquisition oversight functions are added to the process to support analysis necessary for making sound business judgments vis a vis joint C2 conception, design, development, and fielding. Building on Figure 2-5, the emergent structure is illustrated in Figure 3-3.

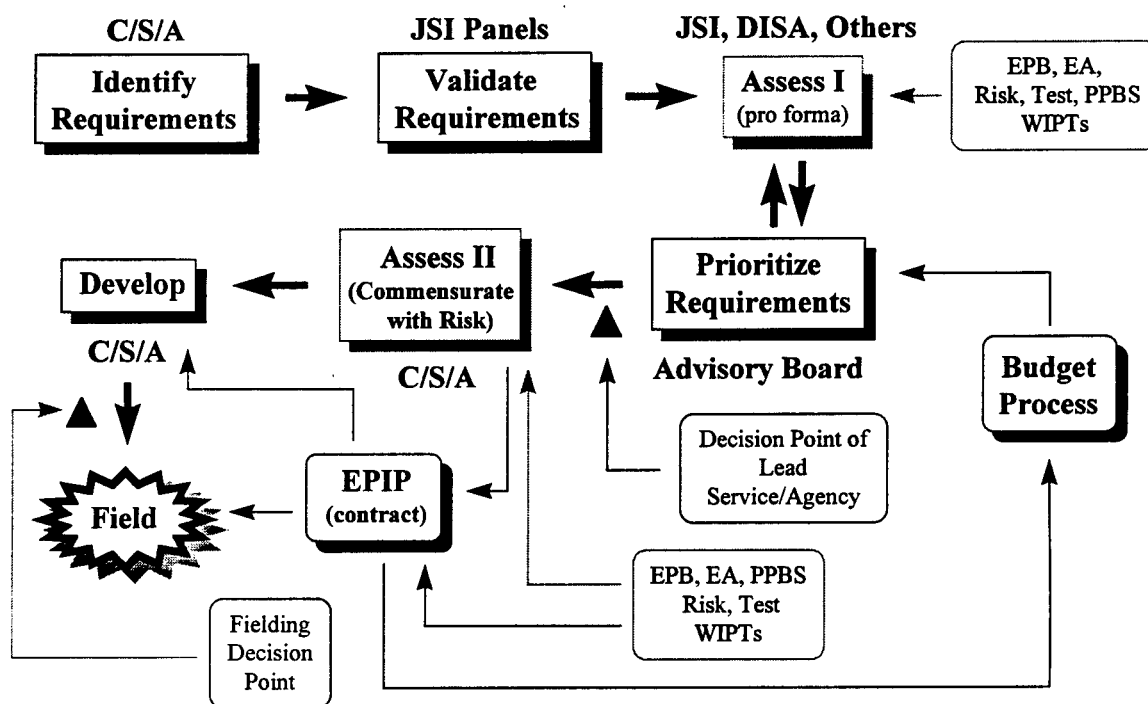


Figure 3-3. United Requirements & Acquisition Oversight Process

2. Roles of Acquisition Oversight WIPTs

Each of the GCCS stakeholder organizations has multiple roles to play in the acquisition process and is represented on a variety of WIPTs. In addition to the JSI Panels involved with requirements identification and validation, there are five standing WIPTs supporting GCCS Acquisition:

- Risk
- Economic Analysis

Test
Budget and PPBS
Evolutionary Build Baseline (Schedule).

Charters for each of these WIPTs are presented below.

To coordinate activities across different WIPT functions, members of the each of the WIPTs belong to the Integrating IPT (IIPT). The purpose of the IIPT is to develop consensus among all GCCS stakeholders, identify issues where closure is not possible, and make recommendations on actions and procedures to the Overarching IPT (OIPT) which is composed of the GCCS stakeholder principals. In turn, in cases where the OIPT does not have sufficient authority to make decisions on GCCS issues, the MAISRC is used to resolve differences and determine ultimate courses of action.

a. Risk WIPT

CHARTER: For each technical solution proposed to satisfy one or more requirement(s), the Risk WIPT identifies those risks that are expected to affect cost, performance, and schedule associated with different options for technical development, implementation, transition, and operations. The Risk WIPT expresses its findings in terms of requirements at risk, their criticality, environment, criteria for success, and fallback options. It assesses the likely impact(s) that a single risk factor, or combination of risk factors, may have on performance, cost, and schedule; it reviews consequences for those who will bear risks identified, including but not limited to users, program management, acquirers, and testers. The Risk WIPT issues guidance to the Economic Analysis, Test, PPBS, and Schedule WIPTs regarding the scope and depth of analysis required to address and remediate identified risks. Organizational representation on the Risk WIPT at a minimum must include: J6 and DOT&E (co-chairs), J3, DISA, other Performer organizations, DTSE&E, PA&E, ASD(C3I), DASD (C3), DASD (C3IA), and any other organization whose responsibilities are substantially affected by changes in risk parameters.

DISCUSSION: A guiding principle of evolutionary acquisition is "emphasis commensurate with risk." Risk assessments provide a basis for determining the intensity of further investigation necessary to ensure that warfighting requirements are properly

identified and ultimately met.⁵ A risk assessment is therefore integral to deciding how to structure economic analyses, tests, schedules, and resource commitments. Figure 3-4 depicts the functioning of risk analyses within the broader Assess I and II frameworks discussed in Chapter 2. Note that an analysis is done for each of the different Segments proposed for an EAP. As will be discussed as part of developing an EPIP, the Segment risk analyses are rolled-up to produce an overall assessment of systemic risk, which is employed to determine the level of testing and depth of economic analysis necessary for the EAP.

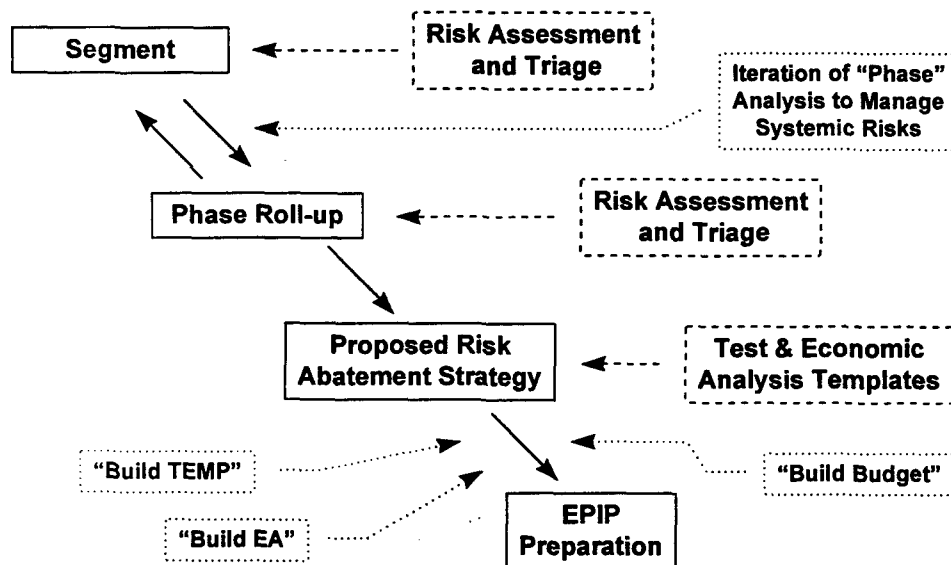


Figure 3-4. Risk Assessment Process

At each stage of the process, a risk assessment and triage are undertaken to determine if the technical and operational risks associated with proposed Segments are bounded and that they are expected to result in acceptable capabilities, functionalities, schedules, and costs. These assessments may employ a variety of formal techniques to array risks against opportunities and needs. Based upon both the individual segment and overall systemic appraisals, a risk abatement strategy is proposed and forms the framework for testing and economic evaluation. The testing framework is subsequently embodied in the Test and Evaluation Master Plan (TEMP) and the EPIP; the economic evaluation forms the foundation for the Evolutionary Phase Baseline (EPB), and along with the EPB is included in the EPIP. It is important to recognize that there are no issues

⁵ GCCS experience has demonstrated that security and transition risks are often significant, widespread, and prolonged for evolutionary programs.

that are out of bounds for the risk analysis. Anything that may have cost, performance, or schedule implications may be addressed. This includes institutional, budget, environmental, force structure, and other matters, as illustrated by Figure 3-5.

b. Economic Analysis WIPT

CHARTER: The Economic Analysis (EA) WIPT assesses the economic consequences of proposed courses of action for affordability, program package definition, identification of alternatives, and POM and budget compliance, and provides decision makers with a complete estimate of costs. The EA WIPT performs two types of economic analyses commensurate with risk. During Assess I, a “rough” analysis is

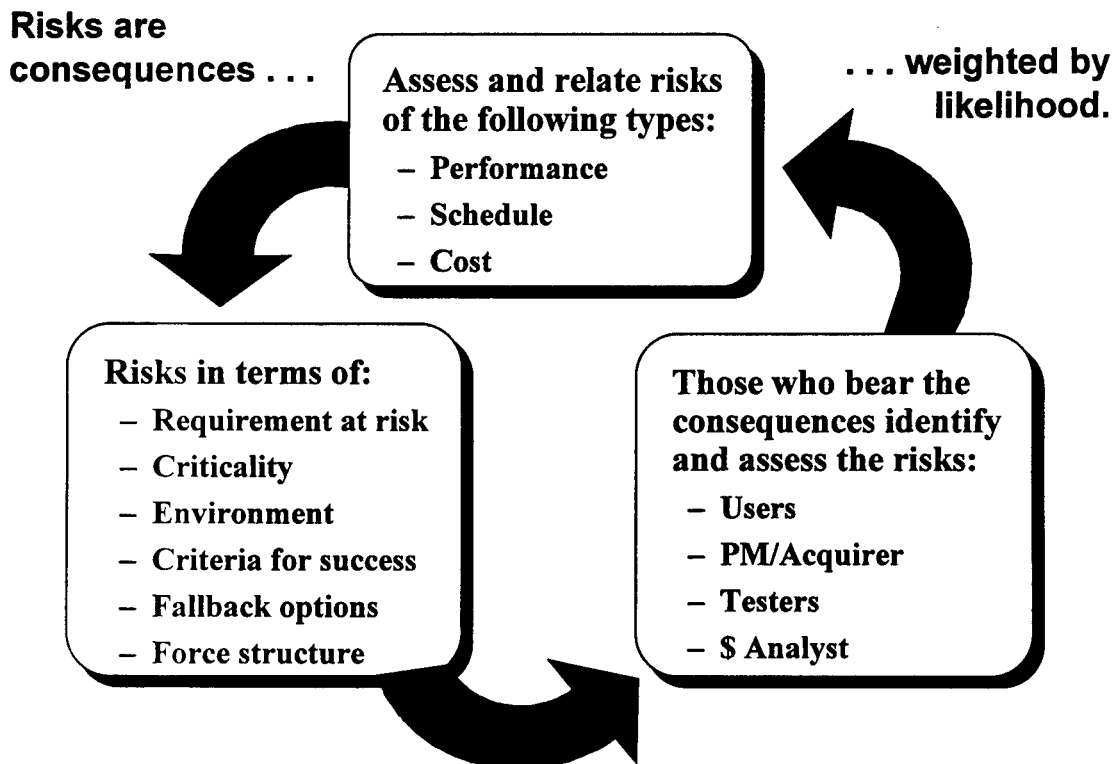


Figure 3-5. Risk Assessment Considerations

conducted to scope costs and economic issues for Segments not yet baselined as part of an EPB. The objective is to provide information to decision makers for use in prioritizing requirements for inclusion in an EAP. During Assess II, a second type of economic analysis is undertaken in support of POM and budget decision activities for baselined Segments. This type of analysis quantifies costs and identifies areas with a high

probability of resulting in baseline breaches. Organizational representation on the EA WIPT at a minimum must include: PA&E and J3 (co-chairs), DISA, other Performer organizations, ASD(C3I), DASD (C3) and any other organization whose responsibilities are substantially affected by changes in economic or cost parameters.

DISCUSSION: Correctly defining the scope for an economic analysis is of particular importance for programmatic success. In the case of the rough analysis, the primary consideration is the identification of any hidden costs that could accrue due to spillover impacts. That is, are the technical and operational implications well bounded and understood so that there will be no unaccounted for "ripple effects" from the fielding of the envisioned capabilities or functionalities? As part of the rough analysis, the EA WIPT identifies and demarcates boundaries used for estimation by assigning cost impacts to one of three categories: GCCS Core; GCCS Core-Related; and GCCS Contingencies (see Figure 3-6).

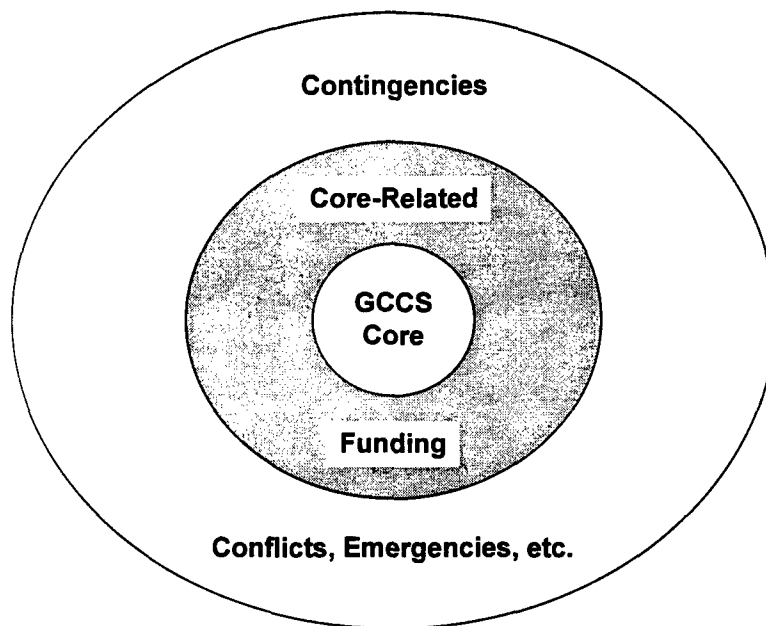


Figure 3-6. Core, Related, and Contingent GCCS Economic Assessments

In the case of the more detailed analysis used to identify resource demands, the central issue is to identify the specific costs and where they will be borne. This is of particular interest to the Services and CINCs since these detailed cost estimates influence the level of funding made available in the future. The Economic Analysis WIPT may direct that other types of assessments be conducted based upon the level of risk associated with individual segments or the overall systemic risk for an EAP.

c. Test WIPT

CHARTER: The test WIPT tailors testing strategies for GCCS EAPs so that they are commensurate with risk, streamlined, flexible, and fully compliant with DoD 5000.2-R. These strategies are mutually agreed upon by the Test WIPT and documented in several plans. At the top, there will be a capstone TEMP for GCCS v3.0 containing the strategy for testing and fielding the core system as well as an annex to this TEMP providing guidance and a format for developing test documentation for future GCCS increments. This guidance conforms to DOT&E's "Guidelines for Conducting Operational Test and Evaluation for Software-Intensive System Increments," dated 1 October 1996. The Test WIPT also helps its members develop test plans and detailed schedules while resolving test resource issues. Organizational representation on the Test WIPT must include: the JITC and J3 (co-chairs), J6, DISA, and any other organization whose responsibilities are substantially affected by changes in test strategy. The OSD testing oversight organizations, DTSE&E and DOT&E, may attend at their own discretion.

DISCUSSION: The primary function of the Test WIPT is to tailor testing objectives and procedures for EAPs commensurate with the technical, operational, and transition risks. The level of testing ranges from a minimum effort for maintenance and application software upgrades; fast-track procedures for mature, low-risk capabilities; focused evaluation of the high risk areas for new, higher-risk segments; quick responses to wartime surges, scale up, or urgent actions; and full DT&E and OT&E for fundamental, system-wide changes.

Testing complements a risk reduction transition strategy for development, integration, implementation, and fielding of new segments as shown in Figure 3-7. The key features of these risk reduction transition steps are the options to proven ability to fall back to a known capability if serious problems arise during testing. These risk reduction features are necessary because the GCCS testing supports an operational fielding decision rather than an acquisition decision as generally assumed in the DoD 5000.2-R process. It also means that avoiding risk to the SOR network requires additional assets to periodically establish a parallel field test network.

Because additional critical functional capabilities are often identified during development itself and because testing complements the risk reduction transition strategy, the full extent of testing required for an EAP is not known until after the EPIP has been

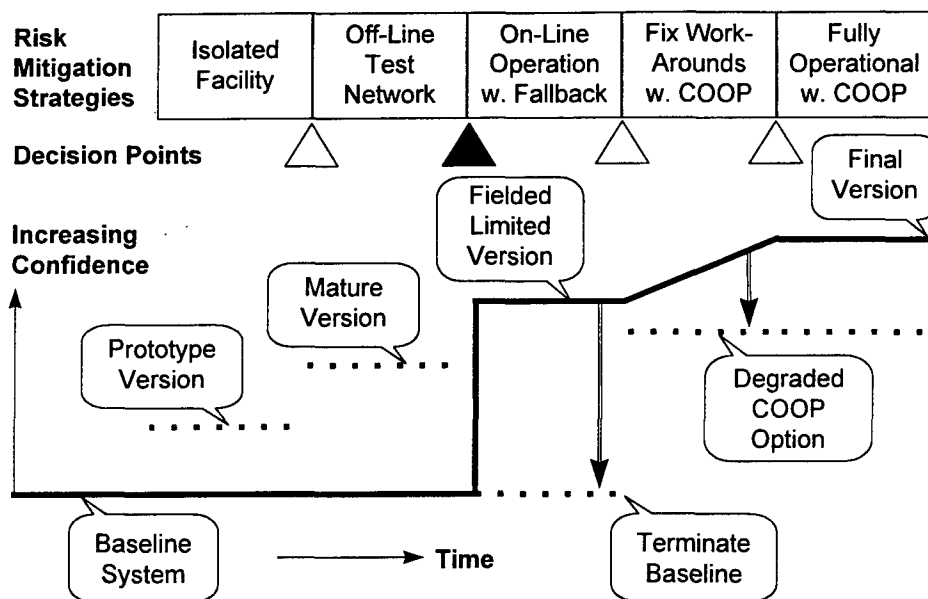


Figure 3-7. Illustration of Transition Steps to Promote Risk Reduction

agreed signed. Therefore, the TEMP Annex to the EPIP must describe the anticipated level of the risk, the corresponding level of testing, and the processes for resolving residual issues as the segment matures. At minimum, it must show a viable transition schedule with supporting test events and decision points. Each decision point should include entrance and exit criteria. These criteria enable the Test WIPT and testers to make dynamic adjustments in the test plans as experience with the maturing system indicates the need for more, or less, additional evaluation. In this way, the TEMP Annex can keep pace with the EPIP approval process while preserving flexibility in the test program. Note that DTSE&E and DOT&E must approve the TEMP Annex to an EPIP, and DOT&E must approve the Operational Test Plans.

d. Budget and PPBS WIPT

CHARTER: The PPBS WIPT issues guidance and recommends procedures for the development of the POM and Service and Agency budgets. It monitors progress on the implementation of ASD(C3I) direction for program element (PE) consolidation for GCCS. This includes the consolidation of PEs for GCCS, including C2 programs supporting GCCS; development of programming and budgeting guidance for GCCS Segments; consideration of PBD-like processes such as the CINC Initiative Fund (expanded or new) and fee-for-service and, assistance to Services and Agencies by providing information necessary for POM submission. Organizational representation on

the PPBS WIPT at a minimum must include: J3 and ASD (C3I) (co-chairs) PA&E, comptroller, J6, DISA, other Performer organizations, DASD (C3), and any other organization whose responsibilities are substantially affected by changes in budget or funding parameters.

DISCUSSION: Securing funding to pursue proposed GCCS technical solutions is perhaps the most complex institutional activity in which GCCS Stakeholders participate. The purpose of the PPBS WIPT is to reconcile these different funding mechanisms and approaches across the Stakeholder Services and Agencies to arrive at a uniform expression of resource needs.

Budget planning for EAPs is undertaken by the PPBS WIPT for forthcoming and future Phases. Because GCCS is an evolutionary program, a modified level of effort approach is used to identify funding requirements within the PPBS process well in advance of each EAP. This is because taking advantage of the rapid progress being made in commercial hardware and software requires a development process that may flexibly adapt to the state-of-the-art as it unfolds.

1. EAP baseline funding is identified through the PPBS process and rooted in a projection of operational requirements to be addressed in the next PPBS cycle. As a result, the PPBS WIPT will identify funding in the Program Objective Memorandum (POM) for activities to be carried out two to four years in the future. Funds so identified and secured form the base level of effort for the program.
2. Prior to the finalization of plans for an EAP, the PPBS WIPT identifies any funding shortfalls relative to evolutionary operational requirements and their respective work packages.

For the upcoming EAP, budget planning consists of a resource allocation process as well as consideration of new requirements that may be above and beyond those envisioned during earlier EAP planning periods. In cases where the ERD identifies new, unenvisioned requirements, the Review Board determines if sufficient resources are available within existing budgets to undertake the additional work. Should this not be the case, the Review Board will recommend to the GO/FO Board one of the following actions:

1. Reprogram funds to undertake the additional work required, including the identification of CINC, Service, Defense Agency, and other organizational resources under the control of GCCS stakeholders that may be voluntarily applied by these organizations against the requirements; or

2. Develop an out-of-cycle budget submission for consideration by the Secretary of Defense to meet the requirements; or
3. Reassess GCCS requirements and priorities, and reschedule activities to minimize potential harm to national security arising from system deficiencies.

e. Evolutionary Phase Baseline (Schedule) WIPT

CHARTER: The Evolutionary Phase Baseline (Schedule) WIPT is responsible for arraying cost and performance against schedule. This includes the development of a master schedule providing general information of long-term plans for GCCS development and implementation, as well as short-term schedules, which are incorporated into the EPIP. The Schedule WIPT also arrays consolidated cost and funding information derived by the EA and PPBS WIPTs according to five-year funding streams. Organizational representation on the Schedule WIPT at a minimum must include: DASD (C3IA) and PA&E (co-chairs), J3, J6, DISA, DOT&E, DTSE&E, other Performer organizations, and any other organization whose responsibilities are substantially effected by changes in schedule parameters.

DISCUSSION: There is no overall acquisition program baseline for GCCS evolutionary acquisition. Instead, there is an evolutionary phase baseline (EPB) for each GCCS EAP. The Schedule WIPT establishes processes for documenting cost, performance, and schedule during planning and execution in an EAP. Each Service or Agency develops Segment information (cost, performance, schedule) which is then rolled up by DISA or the Joint Staff as part of a baseline consolidation process. To complete the implementation plan (EPIP), a schedule of events and anticipated spending streams are developed for assessing resource utilization and direction.

D. SECURITY

GCCS information assurance falls within the purview of the J6. This organization is responsible for developing GCCS security policies and overseeing their implementation. A policy has been established by the J6 for GCCS to identify and protect classified and other sensitive information (see Appendix C). In accordance with national policy, as implemented by DoDD C-5200.10, TEMPEST is to be explicitly addressed early in the EAP planning cycle for all systems that have the potential to emanate sensitive information. A system security engineering management program that

identifies, evaluates, and eliminates or contains system vulnerabilities to known or postulated security threats has also been established.⁶

Interfaces to coalition and non-US civilian activities often are required in crisis operations. Security and security assistance policies are under development for GCCS in conformance with established DoD information assurance practices. This will include the requirement for audit trails and password protection.

The security for GCCS is administered in accordance with the following regulations and instructions:

- DOD Regulation 5200.1, DOD Information Security Program
- DOD 5200.2, DOD Personnel Security Program
- DOD 5200.28, Security Requirements for Automated Information Systems
- DOD C-5200.5, Communications Security⁷

Threats considered include, but are not limited to, the following:

- Physical or electronic attack
- Destruction by national or terrorist entities
- Attempts to capture infosphere elements
- Use of directed energy devices
- Employment of jamming and deception
- Information warfare

Other crisis threats have also been considered, including the environment (e.g., earthquakes, volcanoes). Regional conflicts, the proliferation of weapons of mass destruction, and the possible use of nuclear, chemical, and biological weapons have been considered as factors in crisis planning. Added threats in the event of global war for systems such as GCCS(T) could include nuclear blast, radiation, scintillation, high-altitude electromagnetic pulse (HEMP), antisatellite weapons, and high-altitude nuclear bursts.

⁶ Department of Defense, (11 October 1995), *DoD 5000.2 Instructions*: 4.4.5, Program Protection and Technology Control

⁷ Department of Defense, (May 1995), *Mission Need Statement (MNS) for Global Command and Control System (GCCS)*.

Peacetime threats are also being evaluated and addressed. These include, but are not limited to, the following:

- Foreign intelligence collection
- Intercept/analysis of communications and networks
- Attacks against automated systems and information
- Spoofing

E. IMPLEMENTATION ROLES AND MISSIONS

The EAP implementation process involves six overall missions necessary for the successful fielding and operation of GCCS: testing, training, contracting, software and hardware support services, installation, life cycle support, and transition planning. Any additional or temporary missions not covered here are assigned by the IIPT to a lead organization and may or may not result in the establishment of a working level IPT.

1. Testing

The Joint Interoperability Test Command (JITC) is responsible for conducting and overseeing all GCCS testing. This includes the development of all test documentation and the recording of test results. DISA produces the TEMP or EPIP TEMP annex with test sections written by JITC. JITC also writes the detailed test plans.

2. Training

The development of training plans and oversight for training activities is the responsibility of the J3. This organization identifies the level of training necessary for new functionalities and capabilities to be fielded during an EAP, the resources necessary to support training activities, and timetables adequate to meet the needs of the CINCs.

3. Contracting

All contracting for GCCS is handled by the individual Performer organization and other GCCS Stakeholders on an as needed basis. The specific contracting procedures, rules, and regulations applied to such contracts conform to those of the respective contracting organization.

4. Software and Hardware Support Services

Software and hardware support services for GCCS not contained in the GCCS life-cycle plan, such as help desk and configuration support, are provided by DISA.

5. Installation

The installation of new software and/or hardware due to planned changes in GCCS functionality or capability is provided by DISA.

6. Life-Cycle Support

DISA is responsible for developing and maintaining an up-to-date life-cycle support plan. This plan shall document procedures and for supporting fielded GCCS capabilities.

7. Transition Planning

Transition planning frames and connects all of the above activities. It is used to manage risk under the direction of the Joint Staff, J3. DISA performs planning and coordination activities in support of transition activities. Key considerations include security accreditation, training, documentation, test scheduling, network management, and so forth.

4. EVOLUTIONARY PHASE IMPLEMENTATION PLAN (EPIP) DEVELOPMENT

This chapter describes the process for developing the content of an Evolutionary Phase Implementation Plan. As briefly explained in Chapter 1, an EPIP chronicles and sets forth what will take place during an Evolutionary Acquisition Phase (EAP). It identifies Segments, Stakeholds organizations, funding and resources, deliverables, schedules, support, and testing. In addition, an EPIP sets forth guidelines for oversight, planning, and budgeting activities. The EPIP for Global Command and Control System - "Top Secret," should be referred to as a companion to this Chapter.¹

A. SCOPE OF AN EPIP

An EPIP is not intended to contain all the detailed information necessary to execute the development and fielding of new systems and capabilities during an EAP. Rather, it is intended to be a convenient collection of information regarding activities planned for an EAP. Its role is to provide senior decision makers with a concise description of information necessary for them to make informed decisions and coordinate activities.

To assist decision makers, an EPIP is broken into two parts. A top level EPIP Summary distills information for senior level decision makers. To account for the greater fidelity necessary to carry out an EAP, EPIP annexes contain documents that explain the details of what is to be undertaken and accomplished. In addition, other stand-alone documents, such as Requirements Implementation Documents, are summarized and the longer works incorporated by reference.

Permission to commence work on an EAP is signaled by the GCCS decision authority approval of an EPIP. Such approval, which includes coordination and concurrence among GCCS stakeholders, serves as a declaration that senior management is prepared to commit the necessary funding, time, and resources to accomplish EAP

¹ Richard H. White and David R. Graham, Editors, *Evolutionary Phase Implementation Plan for the Global Command and Control System - "Top Secret" (U)*, Joint Staff, January 1997.

activities. A statement to this effect is generally contained in a preamble to the EPIP Summary.

B. CONTENTS OF AN EPIP SUMMARY

The exact contents of an EPIP Summary vary, along with the complexity, scope, and duration of an EAP. An EPIP consists, at a minimum, of eight parts and associated annexes, as shown in Figure 4-1 (although their arrangement and specific content differ from EAP to EAP). The purpose of the Summary is to provide a convenient distillation of facts and recommended courses of actions for senior level decision makers. In addition to the eight sections shown in Figure 4-1, additional sections may be added to account for special features or characteristics of an EAP. (The EPIP for the Global Command and Control System at the Top Secret level (GCCS(T)) is the model used for Figure 4-1 and is available under separate cover from the Joint Staff.)

The beginning of every EPIP Summary contains a short "authorities preamble" that identifies the decision authorities involved in approving the commencement of an EAP. Since an EPIP is a contract among the participating GCCS stakeholder organizations, it is written in a style similar to that of a legal document.

1. Overview

The Overview section provides a top level summary of the mission and scope of the EAP. This includes general statements of goals contained in the Requirements Implementation Document(s) and what requirements are to be satisfied during the Phase. Mention is also made of EPIP Annexes and stand-alone documents incorporated by reference into the EPIP.

A important part of the Overview section is the explanation of assumptions used as a basis for formulating the document. A clear statement of such assumptions is key to helping decision makers understand what they are signing-up to, and what factors could influence the outcome of an EAP. This section is intended to tell the decision maker that there exists a set of circumstances which could invalidate portions of the EPIP in the areas of cost, performance, and schedule.

EPIP SUMMARY

1. OVERVIEW
 - 1.1 DOCUMENTS INCORPORATED BY REFERENCE
 - 1.2 ASSUMPTIONS
 - 1.2.1 Assumption 1 (Impacts hardware sizing)
 - 1.2.2 Assumption 2 (Impacts network design)
2. DESIGNATION OF LEAD PERFORMER(S)
3. EVOLUTIONARY REQUIREMENTS/TECHNICAL SOLUTIONS
 - 3.1 GENERAL CAPABILITIES REQUIRED
 - 3.2 SPECIFIC CAPABILITIES REQUIRED AND TECHNICAL SOLUTIONS TO BE IMPLEMENTED
 - 3.2.1 JOPES Applications for Deliberate Planning
 - 3.2.2 DSWA and other Requirements
 - 3.2.3 Networking
 - 3.2.4 Security
4. SUPPORT FUNCTIONS
 - 4.1 TRAINING
 - 4.2 INTEGRATED LOGISTICS SUPPORT PLAN
5. RISK OVERVIEW
 - 5.1 TECHNICAL RISKS
 - 5.2 SECURITY RISK
 - 5.3 DEVELOPMENT RISK
 - 5.4 TRANSITION RISK
6. TESTING
7. ECONOMIC ANALYSIS & COST AS AN INDEPENDENT VARIABLE
 - 7.1 STATUS QUO
 - 7.2 ALTERNATIVE 1
 - 7.3 ALTERNATIVE 2
 - 7.4 OTHER CONSIDERATIONS: INDIRECT COSTS & CONTRIBUTION VALUES
 - 7.5 COMPARISON OF ALTERNATIVES
8. EVOLUTIONARY PHASE BASELINE (COST, SCHEDULE, FUNDING)
 - 8.1 SCHEDULE
 - 8.2 COST AND FUNDING

EPIP ANNEXES

- A: Requirements Implementation Matrix
 - B: Technical Concept of Operations
 - C: Functional Description and Technical Architecture
 - D: Security Policy
 - E: Training Plan
 - F: Implementation Plan
 - G: Transition Plan
 - H: Test And Evaluation Master Plan
 - I: Economic Analysis
-

Figure 4-1. Sample EPIP Table of Contents
(Based upon GCCS(T) Phase 1 EPIP)

2. Designation of Lead Performers

The successful execution of an EAP is largely a function of sorting out the roles and missions of the GCCS stakeholders involved in developing and deploying Segments. The section designating Lead Performers calls out the organizations that will execute development activities during the EAP. (Oversight organizations are not referenced in this section.) For each organization referenced, a brief recitation of its roles and responsibilities during the EAP are cited. This may include incorporation by reference of subsidiary documents, including those contained in the EPIP Annexes.

The designation of lead performers is what makes the EPIP into a contract-like instrument. The parties named in this section become bound by the means and objectives set forth in the document. Because an EPIP is a contract, these parties may be seen as "signing-up" to undertake a specified set of activities and will be responsible for delivering according to the schedule contained in the Evolutionary Phase Baseline.

3. Evolutionary Requirements/Technical Solutions

The purpose of this section of the EPIP is to briefly describe the evolutionary requirements to be addressed during the EAP and the technical solutions proposed to meet these requirements. Depending upon the number of organizations involved, the level of resources committed, and the complexity of the tasks involved, requirements and their technical solutions may be discussed on a Segment-by-Segment basis, or grouped according to overarching needs and technical approaches.

Detailed evolutionary requirements are described in the Requirements Implementation Document(s) incorporated by reference into the EPIP, and arrayed for convenience in a Requirements Implementation Summary Annex contained in the EPIP itself. These sources present the specific requirements validated, approved, and prioritized by the Joint Staff. Detailed technical solutions proposed to address these requirements are contained in either a Technical Annex or incorporated by reference into the EPIP from free-standing program documents. In the case of the *GCCS(T) Phase 1 EPIP*, four separate technical Annexes were developed: Technical Concept of Operations, Functional Description and Technical Architecture, Implementation Plan, and Transition Plan.

In addition to requirements provided via RIDs, derivative requirements may also be called out when they are of particular importance. In the GCCS(T) Phase 1 EPIP, for

instance, the networking and security aspects of the system were of sufficient importance that specific needs were discussed in separate sub-sections. This instance demonstrates the need to tailor EPIPs to fit reality and to avoid a one-size-fits-all approach to penning the document.

4. Supporting Functions

The successful operation of fielded capabilities is largely dependent upon the efficacy and efficiency of supporting functions, particularly training and life-cycle logistics support. Whether or not such functions are explicitly made a part of requirements, or regarded as subsidiary considerations, they should be documented in the EPIP summary. In the case of GCCS(T), a decision was made to write a short Training Annex and summarize it in the Supporting Functions section. The Integrated Logistics Support Plan for GCCS(T), however, was incorporated by references and not appended as an annex since it referred to GCCS at both the Secret and Top Secret levels, and was too extensive to warrant simple attachment. Rather, a short sub-section was placed in the EPIP Summary to explain how it applied to GCCS(T).

5. Risk Overview

The GCCS Acquisition Strategy complies with the 5000.2-R ¶ 3.2.2 requirement that every acquisition program establish a risk management program to identify and control performance, cost, and schedule risks via the functioning of its Risk WIPT. As discussed in Chapter 3, the purpose of the Risk WIPT is to identify and track risk drivers, define risk abatement plans, and provide for continuous risk assessment throughout each acquisition phase to determine how risks evolve along with system capabilities and functionalities. Risk reduction measures are included in cost-performance trade-offs, where applicable. The evaluation of risks identifies back-ups in high risk areas and identifies design requirements where performance increase is small relative to cost, schedule, and performance risk.

Generally, considerations of risk are the domain of the Developmental and Operational Test communities. However, in addition to technical risks detailed in test plans, there are a host of programmatic and systematic risks that should be brought to the attention of decision makers as part of a "go/no go" finding. The EPIP Summary should include a brief, general description and assessment of such risks. In the case of GCCS(T), in addition to technical risks, consideration was also given to security risks,

development risks, and transition risks. When necessary, an Annex detailing specific risks should be included to clearly set forth the type and degree of individual and systemic risks anticipated for an EAP. Where possible, risks should be categorized to convey a sense of their importance to the decision maker.

As part of risk management, the length of each EAP is tailored to meet the specific needs of its respective operational requirements and associated Segments. This includes reviewing and assessing the way in which activities are to be conducted, the formality of reviews and documentation, and the need for other supporting activities.

For each EAP, one or more concepts, design approaches, or parallel technologies may be pursued, if warranted, to reduce risk. Prototyping, demonstrations, and early operational assessments are considered and included as necessary so that technological risk is well in hand before the next EAP milestone decision point. Cost drivers, cost-performance trades, and acquisition strategy alternatives should be considered to include evolutionary and incremental software development. The key activities for this phase include identification of risks:

- associated with major cost, schedule, and performance trade-off recommendations;
- of variance with planned cost, schedule, and performance objectives thresholds; and
- of failure for program objectives to be met, and resulting harm to national security.

6. Testing

The development of a Test and Evaluation Master Plan is a central part of oversight activities. Such plans, when properly defined and executed, provide the warfighter with important information regarding the capabilities and limitations of systems fielded. The testing section of the EPIP Summary is used to identify specific test activities that will take place in the developmental and operational arenas. A TEMP Annex shall be incorporated as part of each EPIP. The specific contents of this [test] Annex vary according to the technical and operational challenges as well as the mission criticality of the proposed changes. The level of testing should match the level of challenge posed by the increment. To do this, the Test Annex should follow the guidance and outline provided as Appendix D of this report and a corresponding outline in an annex to the GCCS (3.0) TEMP. Both of these outlines conform to DOT&E's

“Guidelines for Conducting Operational Test and Evaluation for Software-Intensive System Increments” as well as the instructions in DoD 5000.2-R.

For GCCS, developmental testing verifies that the increment satisfies contractual requirements, is mature according to performance metrics, and meets all other conditions necessary to enter operational test and evaluation. Operational testing evaluates whether the increment is operationally effective and suitable to support its mission. To enable operational testers to determine this, users have to identify the critical operational capabilities that must be tested and how well GCCS must perform these capabilities to be ready for fielding as part of the System of Record (SOR). Users can make these identifications in their requirements documents or as subject matter experts (SMEs) assess GCCS performance during DT&E. If performance falls below these user-defined levels, the SMEs will again be asked to identify potential mission consequences and recommend to either fix first the problems or go ahead and field the increment.

7. Economic Analysis and Cost as an Independent Variable

As required by 5000.2-R ¶3.3.3, development of the EPIP incorporates methodologies to acquire and operate affordable DoD systems by setting aggressive but achievable cost objectives and managing achievement of these objectives. These cost objectives are set to balance mission needs with projected out-year resources, taking into account anticipated process improvements in both DoD and defense industries. Known as “cost as an independent variable” (CAIV), this means that cost is considered a constraining factor.

Life-cycle cost-performance trade-offs are considered for each EAP by the EA WIPT, which shall serve as the life-cycle cost-performance integrated product team for GCCS. In this role, the EA WIPT facilitates cost-performance trades, assists the Review Board in establishing program cost-range objectives, and may recommend performance or engineering and design changes as long as the threshold values in the RID can be achieved. If recommended changes require threshold value changes, PA&E as the leader of the EA WIPT will notify the PPBS WIPT and the GO/FO Board. Recommended changes to the EA WIPT will be drafted, where necessary, for approval by the GCCS Decision Authority. The EA WIPT has responsibility for integrating and evaluating all cost-performance trade-off analyses.

Life-cycle cost objectives will be established through consideration of projected out-year resources, recent unit costs, parametric estimates, mission effectiveness analysis

and trades, and technology trends. New and projected sets of life-cycle costs prior to the initiation of each successive EAP will be developed. Requests For Proposals (RFPs) will include cost objectives (as appropriate for the EAP) that provide maximum incentives to the contractor to meet objectives. Whenever applicable, risk reduction through use of mature processes shall be a significant factor in source selection.

A summary of economic analyses conducted as part of defining activities during an EAP should be included in the EPIP Summary. For the purposes of GCCS, a complete economic analysis must contain at least a status quo and one alternative estimate constructed to compare the incremental costs associated with undertaking an EAP. Included with each estimate should be a statement of benefits in qualitative terms, and, where possible, in quantitative terms. At a minimum, the following types of cost impacts are considered as part of any GCCS economic analysis:

- **Hardware Investment:** includes replacement costs for existing equipment, including network-related hardware.
- **Hardware Maintenance:** addresses the costs for maintaining existing equipment, as well as maintenance costs associated with new hardware.
- **Hardware Pre-Planned Product Improvement (P3I):** for evolutionary acquisition P3I is considered identical to hardware investment since EAPs are relatively short and frequent; in general, hardware P3I is shown as part of a periodic replacement cycle.
- **Software Investment:** based upon estimates of the costs associated with developing or reengineering software.
- **Software P3I:** as with hardware, P3I this is a redundant concept for evolutionary acquisition, and such costs are carried as software investment.
- **Training Development:** includes the cost of training materials development for the new operational environment.
- **Phase-Out Operations and Support:** for systems that are to be discontinued, costs associated with phase-out operations and support should be calculated, including costs incurred for parallel operations.
- **Site Operations:** estimates of the costs associated with new operational paradigms, including changes to site configurations, the impacts of new security requirements, and personnel impacts.

As set forth in 5000.2-R, cost parameters include research, development, test and evaluation (RDT&E) costs; procurement costs; military construction costs; operations and maintenance costs; total quantity; and any other cost objectives designated by PA&E (e.g., life-cycle cost objective); all in base year dollars. As GCCS progresses through

subsequent EAPs, procurement costs are refined based on contractor actual (or return) costs from demonstration and validation, engineering development, or prototype deployments. To the extent practicable, cost parameters reflect the total cost of implementation during an EAP and are intended to be realistic cost estimates, based on a careful assessment of risks and realistic appraisals of the level of costs most likely to be realized.

8. Evolutionary Phase Baseline (Cost, Schedule, Funding)

The EPIP shall fulfill the requirements of 5000.2-R ¶2.5 that every acquisition activity establish the basis for fostering greater program stability through the assessment of program cost and determination of affordability constraints. This will be accomplished through a Cost and Affordability Strategy (CAS). Among other considerations, the GCCS CAS includes:

- EAP plans and strategies consistent with overall DoD planning and funding priorities
- Assessments of affordability prior to each milestone decision point (EDR), beginning with IOC
- Provisions for the GO/FO Board to consult with the ASD(C3I) on program objective memoranda and budget estimate submissions that contain a significant change in funding for, or reflect a significant increase in funding.

The Evolutionary Phase Baseline (EPB) serves to combine the results of the economic analysis, budget and resource allocation, and time-line development activities. It details the sources and uses of funds, what activities are to be carried out and when, and ties cost projections back to Program Elements. When taken together with the other portions of the EPIP, the EPB serves a similar role as an Acquisition Program Baseline (APB) as required under 5000.2-R.

Schedule parameters include program initiation, EDRs, initial system of period (SOR), and any other critical system events. These specific other critical events shall be proposed by the IIPT for each EAP.

C. EAP FINALIZATION AND SEGMENT ROLL-UP

Beginning with completed RIDs approved by the GO/FO Board, the Review Board meets to determine, within resource constraints, the operational requirements to be addressed during the forthcoming EAP. This involves translating requirements into

discrete work packages against which funding, personnel, facility, and equipment resources are applied, and for which a work breakdown structure is developed.

The availability of resources determines the level of effort of the EAP, the work packages approved for execution, and the evolutionary requirements addressed during the Phase. The Review Board determines which work packages will be undertaken, based upon an assessment of their priority as assigned by the GO/FO Board, the size of each package relative to funds availability, and the most efficient order for their execution within the overall GCCS mission. Work packages are then scheduled for execution and completion.

For each work package, a design/build/test cycle is defined and used to track progress. Work on each package is electronically recorded and reported on a weekly basis to all GCCS stakeholders via a network planning system maintained by DISA on SIPRNET. This information is used by both the test and acquisition communities to monitor the progress of the EAP, and to schedule testing and milestone reviews.

Consideration of the work packages selected for execution includes:²

- maturity, availability, and applicability of existing commercial and military technologies;
- resource requirements necessary to assure successful design, coding, integration, and testing of system software;
- completion of a test plan based upon realistic expectation of actual, fielded operational performance;
- development of refined program cost estimates, independent cost estimates, and cost objectives;
- development of an updated affordability assessment;
- identification of proposed cost, schedule, and performance objectives and thresholds for approval;
- verification that adequate resources have been programmed to support production, deployment, and support; and
- creation of a proposed oversight and review strategy to include a description of mandatory program information and when this information needs to be submitted for the EAP termination milestone.

² 5000.2

In the course of planning an EAP, a variety of performer organizations may become responsible for developing different Segments. As noted above, the specific roles of each of the performing organizations is called-out in Section 2 of the EPIP Summary, Designation of Lead Performers. This, however, does not answer the question of how the remaining managerial activities for developing cost, performance, schedule, plans, and documentation are carried out.

In order to make GCCS function as a single entity, there is a need to roll-up the disparate activities to be undertaken in any EAP into a single, baselined initiative. This roll-up process constitutes the means by which different performing organizations align their resource needs, development activities, and deployment schedules so that they are arrayed in a logical and efficient manner. The process is illustrated in Figure 4-2.

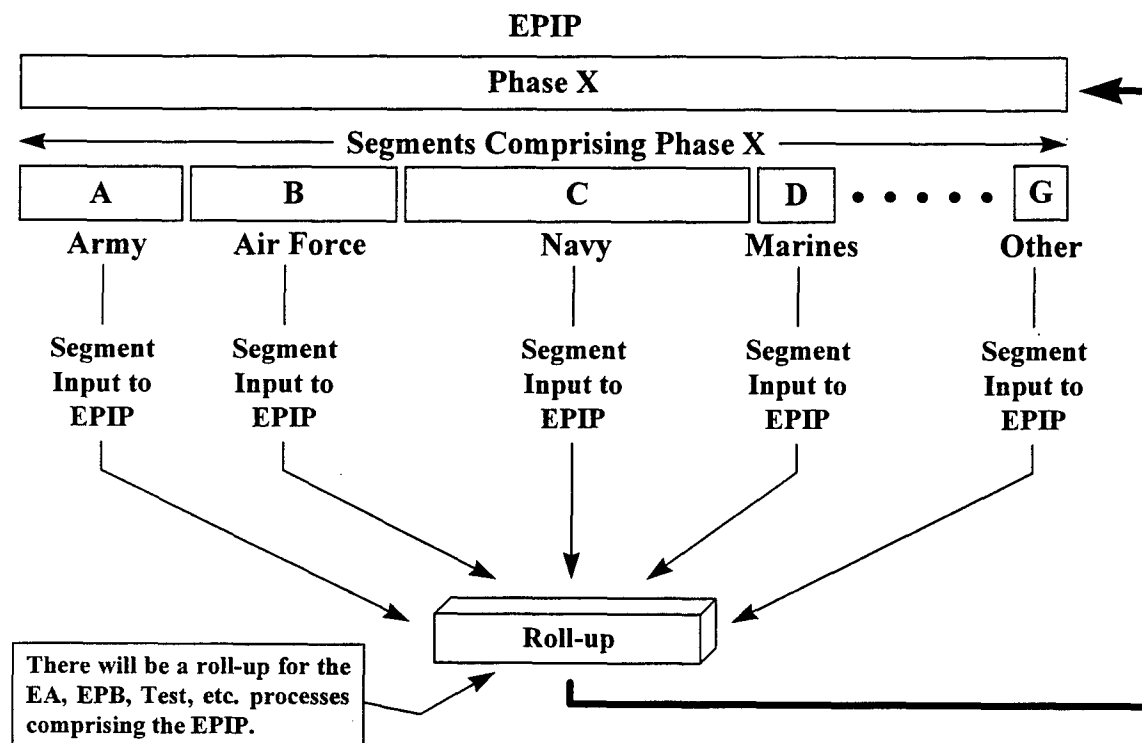


Figure 4-2. Roll-up of GCCS Segments for an Evolutionary Acquisition Phase

Note that the roll-up process takes place separately for each of the elements of an EPIP discussed in Section B, above. That is, each of the responsible performer organizations develops an economic analysis, test plan, budget, and schedule which are combined in the EPIP summary and arrayed along the master schedule time-line. Such a decomposition of EAP activities allows the individual organizations to work according to

their own business practices and within their specific institutional constraints while marching towards a common set of objectives. WIPTs are used on an ad hoc basis to coordinate across activities and facilitate the ultimate roll-up for the EAP.

5. CONCLUSIONS AND RECOMMENDATIONS

In the preceding chapters we described an evolutionary acquisition strategy that addresses the formal coordination and implementation of programmatic activities for the Global Command and Control System. It is important to stress, however, that there are additional issues that must be addressed to make evolutionary acquisition a long-term success for GCCS. Perhaps even more important, for evolutionary principles to become an accepted part of the standard DoD 5000 series approach to acquisition, greater formality must accompany its institutionalization. In this chapter, conclusions and recommendations are provided regarding the general applicability of evolutionary acquisition principles, the need for better evolutionary planning, and the development of a budgeting methodology more suited to the rapidly changing world of information technologies.

A. FORMALIZING EVOLUTIONARY ACQUISITION

The adoption of evolutionary acquisition principles by DoD in the area of information technology is particularly important due to the rapid advance of knowledge and know-how in the domain. It is vital that within such a technologically dynamic environment long-term strategic visions be pursued by adopting a paradigm that in the near-term allows development activities to quickly and flexibly respond to changing customer needs and technological opportunities. A management and planning framework that embraces such principles should be broadly applicable across not only C2 programs, but within the larger Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) realm.

Within DoD, successful adoption of a new paradigm rests largely upon the ability of the Department's leaders to convince those in their chain of command that a new set of initiatives is not merely transitive. The standard approach is to demonstrate commitment by issuing an instruction or regulation which sets forth specific language governing the use and limits of applicability of new principles and procedures. An example of this approach is CJCSI 6721.01, which formally sets forth the GCCS management structure, appointing the J3 the OPR for the activity within the Joint Staff.

For evolutionary acquisition, there does not yet exist a formal document setting forth the way in which the DoD 5000 series acquisition regulations are being interpreted (tailored) for the needs of the C3I (or C4ISR) ¹ community. The preceding chapters provide a guide to the principles and procedures developed for GCCS in this area, but cannot serve as a formal, general statement of policy for the broader community until staffed within the ASD(C3I) organization and approved by the Assistant Secretary.

Recommendation: The ASD(C3I) should review, staff, and formalize the evolutionary acquisition principles developed for GCCS, and provide guidance as to their applicability for other C4ISR programs and activities within his/her purview. Deskbook input specific to automated information systems should be produced that interprets and tailors the DoD 5000 series of acquisition regulations for the C4ISR community. Such input should be submitted to the Defense Acquisition Policy Working Group (DAPWG) for review.

B. IMPLEMENT IMPROVED PLANNING PROCESS

The evolutionary acquisition activities for GCCS to date have, for the most part, involved the development of short-term implementation strategies for joint C2. For GCCS in particular, and to some degree for other C4ISR programs, there remains a need to improve the long-term strategic planning activities involved in deploying advanced information technologies in dynamically changing environments. However, the notion of a long-term plan commensurate with the goals of evolutionary acquisition should not be confused with more traditional long-term strategies for grand design acquisitions.

For evolutionary acquisition to succeed, the strategic planning approach needs to remain extremely flexible. Hence, this task must be approached by developing management and planning tools rather than through formalized projection methodologies. Areas ripe for development include:

- automated configuration management tools to periodically give a snapshot of network and system composition, performance, capacity, and conflicts;
- network, server, and workstation costing models for hardware, software, and firmware;
- facility, staffing, training, maintenance, support, fielding, and upgrading models which provide cost and scheduling estimates; and,

¹ Command, control, communications, computers, intelligence, surveillance, and reconnaissance.

- security analysis tools capable of providing information necessary to perform security risk analyses.

The development of these and related tool sets will allow GCCS managers to quickly identify and respond to technological opportunities within a broader operational framework. A variety of such tools already exists at different stages of maturity; these should form the point of departure for planning framework activities.

Recommendation: The ASD(C3I) should staff an action to identify and select strategic planning tools that will support and comprise a strategic framework for management and planning within the C4ISR environment. The staff should be directed to objectively consider extant tools residing in the government (military and civil) and in the commercial sector (domestic and foreign).

C. REDEFINE BUDGETING APPROACH

The current approach to budgeting for GCCS, and more broadly all C3I programs, is based upon the now obsolescent notion of stovepipe mainframe computing. In the distributed client-server network environment where hardware is rapidly becoming ubiquitous and software machine-independent, there is a need to realign budgeting principles. Such a realignment must be capable of coping with rapid technological changes that are well within current POM planning cycle timelines, as well as the continuous reconfiguration of software systems across an installed hardware base.

In order for evolutionary acquisition to succeed and for funding to be correctly apportioned among DoD C4ISR missions, the Department must begin to account for hardware and software costs on the basis of usage by mission (application) rather than purchase cost. Such an approach could rely upon an internal lease-back style arrangement, a defense working capital fund procedure, pay-per-use scheme, or other accounting methodology. The goal would be to more adequately capture the uses to which equipment is put.

Recommendation: The ASD (C3I) should jointly staff an action with the Director, Program Analysis and Evaluation (PA&E) and the Comptroller to design a new accounting and budgeting methodology more suited to the rapid pace of change in technology and mission area realignment than currently possible within the extant PPBS process.

GLOSSARY

Advanced Technology Demonstration (ATD)
Chief Information Officer (CIO)
Command, Control, Communications, Computing, and Intelligence (C4I)
Command, Control, Communications, Computing, Intelligence, Surveillance,
and Reconnaissance (C4ISR)
Common Operating Environment (COE)
Cost As an Independent Variable (CAIV)
Defense Information Systems Agency (DISA)
Defense Special Weapons Agency (DSWA)
DoD CINCs, Services, and Agencies (C/S/As)
Evolutionary Acquisition Phase (EAP)
Economic Analysis (EA)
Evolutionary Decision Review (EDR)
Evolutionary Phase Baseline (EPB)
Evolutionary Phase Implementation Plan (EPIP)
GCCS Requirements Database (GRiD)
General Officer/Flag Officer (GO/FO)
Global Command and Control System (GCCS)
High-altitude Electromagnetic Pulse (HEMP)
ILS Plan (ILSP)
Integrating Integrated Product Team (IIPT)
Integrated Logistics Support (ILS)
Integrated Product Teams (IPT)
Joint Interoperability Test Command (JITC)
Joint Warfighting Interoperability Demonstration (JWID)
MAIS (Major Automated Information System)
MAISRC (Major Automated Information System Review Council)
MDA (Milestone Decision Authority)
Major Automated Information Systems Review Council (MAISRC)
National Command Authority (NCA)

Office of the Assistant Secretary of Defense, Command, Control, Communication, and Intelligence (ASD/C3I)

Office of Primary Responsibility (OPR)

Office of the Secretary of Defense (OSD)

Operational Evaluation Master Plan (OEMP)

Overarching IPT (OIPT)

Program Analysis and Evaluation (PA&E)

Program Element (PE)

Program Objective Memorandum (POM)

Program, Planning, and Budgeting System (PPBS)

Requirements Implementation Document (RIDS)

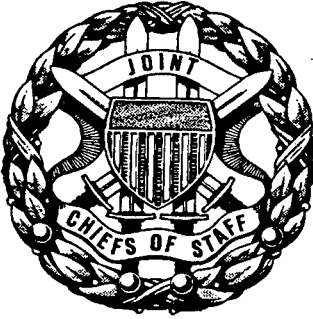
Test and Evaluation Master Plan (TEMP)

Unified Command Plan (UCP)

Video Tele-Conference (VTC)

Working IPT (WIPT)

Appendix A



CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-3
DISTRIBUTION A,B,C,J,S

CJCSI 6721.01
18 February 1995

GLOBAL COMMAND AND CONTROL MANAGEMENT STRUCTURE

1. Purpose. This instruction establishes: responsibilities for the Joint Staff, Services, Defense agencies, combatant and functional unified commands, and other activities regarding management of Global Command and Control (GCC), and a management structure with assigned responsibilities for GCC.
2. Cancellation. The JOPEs Terms of Reference, 29 April 1991, is canceled.
3. Applicability. This instruction applies to the Joint Staff, Combatant and functional unified commands, Services, and Defense agencies.
4. Policy
 - a. The Global Command and Control management structure will provide the C2 oversight to meet the C2 requirements of the NCA, Joint Staff, Service headquarters, combatant and functional unified commands, the Joint Task Force and its components, and DOD agencies. The GCC management structure is established to review, validate, approve, and prioritize requirements and select the best candidate from the nominations for integration into the system, and to approve the policies and procedures that support joint C2 requirements.
 - b. The applications initially incorporated into the Global Command and Control System (GCCS) during the proof of principle period and those that

were picked to create the system baseline were not selected using the procedures described in this management structure. Upon approval of this document, the GCC management structure will govern the selection of applications for integration into GCCS and other systems that support joint C2 requirements. Baseline applications and those subsequently approved for integration may always be reviewed for enhancement or replacement to meet requirements of the functional users.

c. The GCC management structure will establish and maintain liaison with other Defense activities that are engaged in reviews of the systems that support their functional areas. This liaison will ensure that changes to procedures and ADP systems are synchronized, as necessary, with GCCS requirements; that information between functional systems can be exchanged; and that applications warranting integration into the GCCS are identified and incorporated. Liaison will eliminate duplication of effort in the review and selection of applications that meet GCC requirements. The GCC management structure remains the body that approves the selection for migration and integration into GCCS of all ADP applications that satisfy joint command and control requirements.

d. The GCC management structure will manage the implementation of the GCCS and coordinate policy and development functions for GCCS.

e. Existing management structures within the Joint Staff and other organizations currently supporting worldwide C2 systems will be tasked to implement and support the developing GCCS.

5. Definitions

a. Global Command and Control (GCC). GCC encompasses the policies, procedures, trained personnel, and systems that support the C2 of forces, from the NCA through the Joint Task Force and its Service components, during peace, crisis, and war. These policies, procedures, and systems include monitoring, planning, and executing mobilization, deployment, employment, sustainment, redeployment, and force regeneration activities associated with military operations.

b. Global Command and Control System (GCCS). A comprehensive, worldwide network of systems which will provide the NCA, Joint Staff, combatant and functional unified commands, Services, Defense agencies,

Joint Task Forces and their Service components, and others with information processing and dissemination capabilities necessary to conduct C2 of forces. GCCS is a means to implement the Command, Control, Communications, Computers, and Intelligence for the Warrior (C4IFTW) concept. An evolutionary implementation strategy is being used to provide warfighters with their required operational capabilities. The GCCS no grand design philosophy lends itself to extensive user participation, incremental fielding, and shorter periods between update cycles.

6. Responsibilities. Responsibilities of the Chairman of the Joint Chiefs of Staff, the Office of Primary Responsibility (OPR), the GCC General/Flag Officers Advisory Board, the GCC Review Board, the Functional Area and Systems Integration Working Groups, the Joint Staff, the Combatant and functional unified commands, the Services, the Defense Systems Information Agency, and other DOD agencies are listed in Enclosure A.

7. Procedures. Procedures applicable to the GCC management structure are incorporated within the responsibilities of the OPR, the General/Flag Level Advisory Board, the GCC Review Board, the Functional Area and C4 Systems Integration Working Groups, the Joint Staff directorates, combatant and functional unified commands, Services, and DISA.

8. Effective Date. This instruction is effective upon receipt.

For the Chairman of the Joint Chiefs of Staff:

Enclosures:

A--Responsibilities

B--Management Structure Diagram

CJCSI 6721.01
18 February 1995

(INTENTIONALLY BLANK)

ENCLOSURE A

RESPONSIBILITIES

1. Chairman of the Joint Chiefs of Staff. The CJCS is responsible for policy guidance and oversight of GCC. His guidance is transmitted to the Director, Joint Staff, for implementation.
2. Office of Primary Responsibility (OPR). The Director for Operations, J-3, Joint Staff, is the OPR for this instruction.
 - a. The Director, J-3, is also responsible for development of GCC CONOPS, policy, and functional requirements.
 - b. The OPR:
 - (1) Approves the GCCS Planning and Program Budget System (PPBS) submissions for those funds managed by the Joint Staff and DISA. Receives for information the Services' GCCS spending plans and PPBS submissions that support Joint and Service GCCS requirements, to include modifications to those applications that have been integrated into GCCS; for applications that are planned to migrate to GCCS; and for applications that meet the requirements in subparagraph 5b.
 - (2) Approves the development and implementation plans for the processes and capabilities that support GCC.
 - (3) Approves GCC policy in accordance with guidance from the Chairman of the Joint Chiefs of Staff.
 - (4) Directs revisions to the current planning and execution procedures to match current national strategy and the Unified Command Plan (UCP). The Director, J-3, will ensure the GCC development strategy is consistent with changes to current planning and execution.
 - (5) Serves as chairperson of the GCC Flag/General Officer Advisory Board.

c. The OPR is assisted by the following management structure:

- (1) The GCC General/Flag Officer Advisory Board.
- (2) The GCC Review Board.
- (3) The GCC Functional Area and C4 Systems Integration Working Groups.

3. GCC General/Flag Officers Advisory Board. The Director, J-3, is the chairperson. Members of this board consist of flag officers or their flag level representatives from all Joint Staff directorates, Services, combatant and functional unified commands, and DISA. Other DOD agencies will be invited to attend as appropriate to the agenda topics. The board meets quarterly, or as directed by the chairperson. The board will:

- a. Advise the OPR on priority and execution of GCC requirements, policy, and development and implementation plans.
- b. Provide the CJCS, Services, combatant and functional unified commands, and the Joint Staff with information concerning GCC requirements, objectives, and milestones.
- c. Ensure that Service coordination is accomplished on those actions affecting budgeting and resources.
- d. Identify, discuss, and take action on any unresolved GCC issues and recommendations forwarded by the GCC Review Board or presented by a member of the General/Flag Officers Advisory Board.
- e. Approve new functionality to be developed or included into GCCS.

4. The GCC Review Board. This board reviews GCC requirements and issues, forwarding those requiring action to the General/Flag Officers Advisory Board with recommendations and executing those actions consistent with OPR-approved development and implementation plans.

a. Composition of the Board. The Vice Director, J-6, will chair the review board. Members to this board consist of O-6 representatives from all Joint Staff directorates, Services, combatant and functional unified commands,

and the chairs from the functional and Systems Integration Working Groups. Other DOD activities will be invited to attend as appropriate to the agenda. The board will meet quarterly, or as required by the chairperson.

b. Responsibilities

(1) The GCC Review Board is the primary body charged with consolidating, validating, and directing the implementation of GCCS requirements. The board will:

(a) Direct the execution of those validated requirements that support the OPR approved development and implementation plans.

(b) Approve those applications that compete as part of the GCCS best-of-breed process. The review board evaluates the technical, functional, training, and funding criteria in determining which application is selected to satisfy identified requirements. Applications that support approved development and implementation plans will migrate to GCCS. Applications that support GCC requirements, but which do not have approved plans, will be forwarded with prioritized recommendation to the General/Flag Officer Advisory Board.

(2) Periodically reviews and forwards to the General/Flag Officers Advisory Board the status of the DISA funding expenditures for execution of GCCS requirements.

(3) Reviews and forwards for action to the General/Flag Officers Advisory Board the development and implementation plans for those systems or applications that support GCC.

(4) Reviews other GCC issues, forwarding those of interest or requiring OPR decision to the General/Flag Officers Advisory Board.

(5) Reviews and approves Functional Area and C4 Systems Integration Working Group charters, as submitted.

- (6) Reviews functional improvements and other proposals proposed by the Functional Area and C4 Systems Integration Working Groups. It also executes those proposals that are consistent with approved development and implementation plans. It forwards with recommendation to the General/Flag Officers Advisory Board those proposals that were not considered during the creation and approval of the GCCS development and implementation plans. It coordinates and prioritizes working group recommendations and provides user feedback on General/Flag Officers Advisory Board recommendations and OPR implementation decisions.
- (7) Provides direction and oversight to the Functional Area and C4 Systems Integration Working Groups.
- (8) Reviews and approves GCC procedures.
- (9) Reviews and forwards GCC policies submitted by the Functional Area and C4 Systems Integration Working Groups to the General/Flag Officers Advisory Board for OPR approval.
- (10) Directs as necessary the creation of ad hoc action officer working groups with planner-level involvement as required to examine issues falling outside the purview of the established working groups.
- (11) Ensures horizontal coordination of proposed functional improvements between all functional area and C4 Systems Integration Working Group panels.

5. Functional Area and Systems Integration Working Groups. The following Functional Area and Systems Integration Working Groups will operate in accordance with the general instructions outlined in paragraph 6 of this enclosure. Membership will be determined by the working group. At a minimum, each group will include representatives in grade of O-5 or below from the Joint Staff directorates, Services, combatant and functional unified commands and/or their component commands, and DOD agencies. A member from the Joint Staff chairs each working group. The working groups may extend co-chair responsibilities to representatives from the combatant and functional unified commands and/or Services as they determine appropriate.

- a. GCC Intelligence Functional Area Working Group. A representative from the Director, J-2, Joint Staff, is the chairperson. The group executes those responsibilities defined in paragraph 6 of this enclosure and is responsible for all areas and issues relating to intelligence.
- b. GCC Employment and Crisis Action Functional Area Working Group. A representative from the Director, J-3, Joint Staff, is the chairperson. The group executes those responsibilities defined in paragraph 6 of this enclosure and is responsible for all areas and issues relating to employment.
- c. GCC Sustainment Functional Area Working Group. A representative from the Director, J-4, Joint Staff, is the chairperson. The group executes those responsibilities defined in paragraph 6 of this enclosure and is responsible for all areas and issues relating to sustainment, force regeneration, mobilization, and demobilization.
- d. GCC Deployment/Redeployment Functional Area Working Group. A representative from the Director, J-4, Joint Staff, is the chairperson. The group executes those responsibilities defined in paragraph 6 of this enclosure and is responsible for all areas and issues relating to deployment and redeployment.
- e. GCC C4 Systems Integration Working Group. A representative from the Director, J-6, Joint Staff, is the chairperson. The group executes those responsibilities defined in paragraph 6 of this enclosure and is responsible for all areas and issues relating to C4 systems integration. The Working Group coordinates its oversight efforts with the GCCS Project Manager (PM) to avoid duplication of effort, focusing its work on providing GCCS development requirements to the GCCS PM. In addition, the group executes the following additional responsibilities:
 - (1) Maintains oversight of design, development, acquisition, and integration of the hardware and software automated systems that support GCCS requirements, including configuration management, communications management, data administration, information security, and operations and maintenance of the GCCS network.
 - (2) Integrates ADP requirements from other GCC functional working groups.

- (3) Assists functional and ad hoc working groups to develop transition and migration plans.
- (4) Consolidates and integrates technical requirements and attributes with approved functional requirements to establish an overall C2 capability.
- (5) Coordinates staffing and review of specification documentation and prototypes with the Services, combatant and functional unified commands, DOD agencies, and the Joint Staff.
- (6) Coordinates GCCS interfaces with other DOD and non-DOD agencies.
- (7) Explores commercial-off-the-shelf (COTS) automated systems and communication services and Government-owned system interfaces.
- (8) Identifies functions, current system functional performance levels, and functional performance specifications and requirements. Forwards requirements through the management structure to the GCCS PM.
- (9) Provides liaison to other working groups to ensure requirements are integrated as required into the GCCS strategy.
- (10) Receives updates and requirements from functional working groups with specific mapping and graphics requirements.
- (11) Incorporates information security systems, policies, and guidance.
- (12) Includes corrections and modifications incorporated in fielded versions, in accordance with assigned priorities.
- (13) Serves as the GCC liaison to the Military-Communications Electronic Board (MCEB), attending all MCEB meetings and reporting on matters of interest to the GCC management.

(14) Maintains liaison with the GCCS Common Operating Environment (COE) working group, ensuring incorporation of identified GCCS technical requirements.

(15) Coordinates the activities of the subworking group on GCCS Security.

f. GCC Deliberate Planning Working Group. A representative from the Director for Operational Plans and Interoperability, J-7, Joint Staff, is the chairperson. The group executes those responsibilities defined in paragraph 6 of this enclosure and is responsible for all areas and issues relating to deliberate planning. Also, the group:

(1) Prepares joint publications that describe GCC procedures used to support joint operation planning, such as JOPES.

(2) Integrates, in conjunction with the Employment and Crisis Action Working Group, joint doctrine crisis action policies and procedures with deliberate planning policy and procedures.

(3) Reviews those policies and procedures identified by other GCC working groups to ensure interoperability and integration within GCC policies.

(4) Documents and integrates procedural changes associated with fielding new GCCS automated processes.

g. GCC Training Working Group. This working group is co-chaired by representatives from the Director, J-3, and the Director, J-6, Joint Staff. In addition to those members defined in paragraph 6 who are routinely invited, membership is extended to those organizations that support GCCS technical training and training of those applications that migrate to GCCS. The GCC Training Working Group identifies training requirements to support transition and sustainment training of those applications that are selected for migration to GCCS, and determines the resources required to support GCCS training.

h. GCC Readiness Working Group. A representative from the Director, J-3, Joint Staff, is the chairperson. The group executes those responsibilities

defined in paragraph 6 of this enclosure and is responsible for all areas and issues relating to readiness.

i. GCC Modeling and Simulation Working Group. A representative from the Director, J-8, Joint Staff, is the chairperson. The group executes those responsibilities defined in paragraph 6 of this enclosure and is responsible for all GCC areas and issues relating to modeling and simulation.

j. Ad hoc Working Groups

(1) Chairperson. As determined by the GCCS Review Board or the OPR.

(2) Membership. As determined by the chairperson and guidance from the convening authority.

(3) Responsibilities. As determined by the chairperson and guidance from the convening authority.

6. Functional Area and C4 Systems Integration Working Groups--General Responsibilities. Permanent Functional Area and Systems Integration Working Groups will be established in those areas that are routinely involved with GCC. Ad hoc working groups can be created to examine specific issues that do not clearly belong to one of the permanent functional area working groups. The Joint Staff directorate that provides the Functional Area and C4 Systems Integration Working Group chair is also responsible for providing required support to ensure the group can accomplish its assigned and implied taskings. Working groups meet as frequently as required to accomplish their objectives. All Functional Area and C4 Systems Integration Working Groups are organized similarly and execute the following responsibilities:

a. Chaired by a Joint Staff and/or appropriate combatant command representative at the planner level.

b. Conduct working sessions with functional representatives to review status of work, priorities, and milestones.

c. Develop and maintain a functional area plan for developing GCCS requirements.

- d. Conduct front-end analysis of functional objectives. Sponsor prototype development and obtain functional user involvement throughout the requirement refinement process in accordance with standards identified by the GCCS PM. Responsible for developing functional area requirements and identifying best of breed applications to satisfy those requirements. Groups will ensure that operational user input is obtained while developing and refining GCCS strategies, objectives, requirements, and priorities, and provide users feedback concerning identified requirements.
- e. Identify policies and procedures that are necessary to execute their respective functional areas. Policy changes will be staffed by the Joint Staff directorate that furnishes the working group chair and will be approved by the OPR. Procedures will be staffed by the working group and are forwarded to the GCC Review Board for review and approval. Upon approval of procedural and policy changes, the responsible working group will coordinate with the Joint Staff Doctrine Division and the appropriate Joint Staff directorates to ensure that changes are annotated in Joint Staff doctrine and publications.
- f. Review development and implementation activities to ensure that GCC strategies, requirements, and priorities are being met in their functional areas.
- g. Evaluate ADP applications and interfaces that meet specific functional area requirements. Provide approved requirements to the C4 Systems Integration Working Group for development, fielding, and maintenance and to the Training Working Group for transition training support.
- h. Identify and provide a knowledgeable team of user representatives who will provide liaison with software developers throughout the development, testing, and fielding process of GCCS software and hardware applications. Provide all necessary liaison to other working groups to ensure the working group's requirements are integrated into GCCS development. Provide a mechanism to ensure that user feedback is maintained throughout the process, from requirements identification through fielding of migration candidates and applications.
- i. Identify data requirements to the C4 Systems Integration Working Group for identification and integration into GCCS data administration. Coordinate with appropriate Service/CINC to ensure live data feeds for

existing data flows are transmitted and procedures written to require transmission of new data from the source. Identify required additions and changes to data element standards in the working group's area of responsibilities.

j. Respond to OPR and GCC Review Board taskings through the appropriate chain of command and administrative support structures.

k. Provide progress reports through the GCC Review Board to the General/Flag Officers Advisory Board as required.

l. Identify functional and technical training requirements for GCCS and submit them to the Training Working Group.

m. In conjunction with the C4 Systems Integration Working Group, identify requirements and develop a plan to ensure their transition from the current systems supporting the functional area to GCCS. Submit plans to the GCC Review Board for consolidation and submission to the General/Flag Officers Advisory Board for OPR approval.

n. Ensure that security requirements, including hardware and software technology transfer and data responsibility, are considered when identifying, reviewing, and refining functional requirements.

o. Develop charters and submit for approval to the GCC Review Board.

7. Joint Staff. Through the appropriate Functional Area and C4 Systems Integration Working Group, Joint Staff directorates will participate in actions to accomplish the following: review and collaborate on GCCS documentation and prototype review; define and develop specific GCCS requirements that fall in the directorates' areas of functional responsibilities; resolve issues relating to standardization of functional data elements to be used in GCCS; and coordinate with the OPR on developing, testing, and implementing GCCS capabilities. Each Joint Staff directorate provides a flag level representative to the General/Flag Officers Advisory Board, a planner level representative to GCC Review Board, a planner as chairperson of the Functional Area Working Group(s) for which it is responsible, and representatives to other established and ad hoc working groups as required. Each Joint Staff directorate assists the OPR in all GCC matters and serves as the Joint Staff point of contact for all GCC matters related to the directorate's area of responsibility. All Joint Staff directorates will identify and

initiate staffing on modifications of policy, procedures, and the Joint Reporting System (JRS) as an integral part of GCCS development.

a. Director for Manpower and Personnel, J-1. The Director, J-1, will assist the OPR by exercising responsibility for all GCC issues relating to personnel support systems.

- (1) Identifies personnel support system requirements.
- (2) Provides staff expertise to the appropriate functional working groups to support development of systems that meet identified requirements.

b. Director for Intelligence, J-2. The Director for Intelligence, J-2, will assist the OPR by exercising oversight of intelligence systems development, integration, and management of intelligence automated information activities in GCCS including integration of non-DOD intelligence community systems.

- (1) Serves as the Joint Staff point of contact in all intelligence systems matters.
- (2) Provides the chair for the Intelligence Functional Working Group.
- (3) Assists the OPR by coordinating with ASD(C3I), the Intelligence Systems Board and the Intelligence Community Management Staff on intelligence systems matters.
- (4) Assists the OPR by executing oversight of standards, interoperability, and requirements for intelligence applications within GCCS.
- (5) Represents the Combat Support Intelligence Agencies for GCC matters.

c. Director for Operations, J-3

- (1) Exercises functions of OPR, maintaining oversight of all aspects of GCC policy, procedures, development, implementation, funding within

the scope of CJCS guidance, and chairing the GCC General/Flag Officer Advisory Board.

- (2) Serves as the GCC Functional Manager, responsible for coordination of system-wide functional requirements.
- (3) Reviews deployment and crisis action planning policy and procedures.
- (4) Approves GCC policy.
- (5) Approves GCCS spending and PPBS submissions of those funds managed by the Joint Staff and DISA. Receives for information from the Services their GCCS spending and PPBS submissions.
- (6) Approves GCCS development and implementation plans.
- (7) Provides the chairperson for the Employment and Crisis Action Functional Area Working Group, the Readiness Working Group, and the co-chairperson for the GCC Training Working Group.
- (8) In coordination with J6, exercises oversight of GCC training, with responsibility for functional training.
- (9) Coordinates GCC training in the National Capital Region, to include Flag and General officer seminars.
- (10) Maintains a GCC Support Branch to serve as the administrative liaison between the OPR and the users.

d. Director for Logistics, J-4. The Director for Logistics, J-4, will assist the OPR by exercising responsibility for mobilization, demobilization, sustainment, reconstitution, deployment, and redeployment policy and procedure definition, and for management of related prototype development efforts. Specific roles include working with the CINCs to clarify and define customer requirements, working with the Services and Defense agencies to develop policies and procedures for satisfying these requirements, and identifying those logistic automated information systems that must be interfaced (or interoperable with) to provide accurate and timely information. Functions include:

(1) Serving as the Joint Staff point of contact in all logistics Information System matters pertaining to mobilization, demobilization, deployment, redeployment, sustainment (including medical), and reconstitution.

(2) Providing chairs for the Sustainment, and Deployment and Redeployment Working Groups (and subgroups as required) within GGCS.

(3) Defining and refining logistics information system mobilization and sustainment policies, procedures, and ADP support requirements in collaboration with the logistics staffs of the Services, combatant and functional unified commands, and Defense agencies.

(4) Preparing input to appropriate documentation.

e. Director for Strategic Plans and Policy, J-5. The Director for Strategic Plans and Policy, J-5, serves as the Joint Staff point of contact for GCC coordination with DOS, CIA, FEMA, and other non-DOD agencies.

f. Director for Command, Control, Communications, and Computer Systems Directorate, J-6

(1) Assists the OPR by serving as system implementer executing technical oversight for all C4 system development, ADP integration and management of technical activities in GCCS, operations and maintenance of the network, data administration, configuration management, and communications management.

(2) Directs the design, development, acquisition, and integration of automated systems that support OPR-approved GCC requirements and provides this plan to the OPR for approval.

(3) Provides the OPR with a technical impact assessment on proposed functionality changes.

(4) Coordinates technical hardware development and integration with the Services to ensure required support is present when GCCS

software is fielded. To this end, identifies and coordinates with the Services total resource requirements to support GCCS.

(5) Prepares and reviews, in conjunction with DISA, the spending and PPBS submissions of those funds managed by the Joint Staff and DISA that support development and implementation of systems that support GCC. In conjunction with the OPR, approves the GCCS spending and PPBS submissions. In conjunction with the OPR, receives for information the Services and other DOD agency GCCS spending and PPBS submissions. Executes the budget approved by the OPR that is required to support development, testing, fielding, acquisition, and initial maintenance of GCCS hardware, operating software, and ADP applications. Advises the OPR of funding constraints that may affect satisfying GCCS requirements and milestones. Submits changes to the approved spending and development plans for OPR concurrence.

(6) Identifies, in conjunction with the Services, Service resource management and budgeting requirements in support of GCCS.

(7) Directs the preparation of development and implementation and executes those plans approved by the OPR.

(8) Assists the OPR by coordinating with ASD(C3I) for acquisition matters.

(9) Provides necessary guidance and direction to DISA/PM GCCS to execute development, evaluation, acquisition, fielding, maintenance, and configuration control of GCCS COE interfaces and GCCS applications.

(10) Performs duties as GCCS data administrator, including approval of data element standardization for compliance with DOD standards. Approves data standardization policy for GCCS to resolve data base compliance.

(11) Executes oversight of GCCS configuration management.

(12) Approves Joint Reporting System changes in accordance with Joint Pub 1-03.

- (13) Serves as the Joint Staff point of contact for all GCC matters relating to C4.
- (14) Manages, in coordination with J-3, oversight of GCCS training, with responsibility for technical training.
- (15) Coordinates with the OPR those COTS automated systems, telecommunication services, and Government-owned system interfaces as technical solutions that support GCCS requirements.
- (16) Provides oversight of the network management of the operational system supported by DISA.
- (17) Coordinates technical decisions with the GCC Review Board to avoid adverse impact on users.
- (18) Provides the chairperson of the C4 Systems Integration Working Group, and provides the co-chairperson for the GCC Training Working Group.
- (19) Publishes the agenda and minutes of the GCC Review Board.
- (20) Ensures, in the capacity as the chairperson of the MCEB, that issues of interest to the GCC management structure are presented to this body, and that issues emerging from this group are identified to the GCC management structure.
- (21) Provides flag-level chair to the GCC Review Board.

g. Director for Operational Plans and Interoperability, J-7

- (1) Assists the OPR by executing responsibility for development, integration, and documentation of GCCS procedures.
- (2) Reviews development of deliberate planning policy and procedures.
- (3) Exercises primary Joint Staff action for the publication and continuing development of the policies and procedures for the review of the operation plans of combatant and functional unified commands.

- (4) Provides observers and participants to attend deliberate planning conferences.
- (5) Assists the OPR in all GCC matters relating to development of deliberate planning procedures.
- (6) Serves as the Joint Staff point of contact for all matters relating to GCC deliberate planning procedures.
- (7) Provides chairperson for the Deliberate Planning Working Group.

h. Director for Force Structure, Resources, and Assessment, J-8

- (1) Coordinates with the OPR to determine the GCCS effect on modeling and simulation results.
- (2) Coordinates with the OPR on the development and employment of C4 analytical models.
- (3) Serves as the PPBS advisor for GCCS matters.
- (4) Establishes modeling and simulation interface requirements for GCCS.
- (5) Provides the chairperson for the GCC Modeling and Simulation Working Group.

8. Combatant and functional unified commands

- a. Provide flag-level representatives to the GCC General/Flag Officers Advisory Board.
- b. Provide 0-6 representatives to GCC Review Board.
- c. Provide representatives to Functional Area and C4 Systems Integration Working Groups and provide representatives with CJTF staff expertise to the Employment and Crisis action working group.

- d. Attend other working groups as required.
- e. Provide emerging requirements to appropriate working groups for action and, as required, provide test bed for GCCS prototypes.
- f. Oversee, in coordination with the Services, the operation and maintenance of the GCCS sites.
- g. Establish, at discretion, an ad-hoc working group with membership that represents functional area mission requirements. This group will ensure information from the GCC working groups is spread throughout the command, and be able to provide current information to the CINC planners and general officers who attend the Review Board and General/Flag Officers Advisory Board.

9. Military Services

- a. Provide a flag-level representative to the GCC General/Flag Officers Advisory Board.
- b. Provide 0-6 level representatives to GCC Review Board.
- c. Provide representatives to Functional Area and C4 Systems Integration Working Groups.
- d. Establish Service GCCS points of contact for planning and coordinating functional and technical Service efforts related to GCCS development and resources.
- e. Plan, program, and budget, upon identification of specific requirements (within fiscal constraints), the resources required to support the following:
 - (1) Changes to their existing systems that provide data to GCCS.
 - (2) Fielding, operations, maintenance, and training at designated Initial Operational Capability (IOC) and Service selected sites after delivery of DISA provided IOC hardware/software and subsequent system and application upgrades.
 - (3) Necessary internal initiatives.

- f. Provide for information to the Joint Staff J-3 and J-6 Service GCCS spending plans and PPBS submissions that support Joint and Service GCCS requirements, to include modifications to those applications that have been integrated into GCCS; for applications that are planned to migrate to GCCS; and for applications that meet the requirements in subparagraph 5b.
- g. Operate and maintain, in coordination with the combatant and functional unified commands and components, GCCS sites.
- h. As members of the GCC Review Board and the General/Flag Officers Advisory Board, serve as channels for providing the Services information about proposed GCCS activity that may impact Service resources and POMs. Decisions affecting Service resources and POMs will be staffed through normal Service coordination procedures.

10. Defense Information System Agency (DISA)

- a. Serves as executive agent of the Joint Staff for GCCS and for the transition efforts that migrate current systems to GCCS.
- b. Provides the Project Manager for GCCS who provides oversight and direction of activities in DISA to:
 - (1) Integrate, test, and field all GCCS ADP applications in accordance with Joint Staff guidance.
 - (2) Develop and maintain GCCS configuration management with direct user involvement in accordance with the DISA configuration management policy.
 - (3) Provide periodic updates to the GCC General/Flag Officers Advisory Board on program development and budget execution.
 - (4) Coordinate staffing of specification documentation, prototypes, and other system improvements with the Services, combatant and functional unified commands, other Defense agencies, and the Joint Staff. Provide version content documents to the Working Groups and the engineering analysis for nominated functions.

(5) Provide J-6 a technical impact assessment on proposed new functionality. Advise the J-6 of technological and financial constraints that may adversely affect achieving GCCS requirements and milestones.

(6) Develop specific application software as approved by the GCC OPR and directed by the J-6.

(7) Incorporate approved Engineering Change Proposals (ECPs) and Incident Reports (IRs) into the GCCS baseline.

(8) Provide the technical oversight and participate, as appropriate, in all GCCS testing efforts.

(9) Provide appropriate and necessary functional and technical documentation for ADP applications.

(10) Develop funding estimates that support GCC requirements and align funding to support the approved GCCS development and implementation plans. Provide these estimates and proposed allocation of funds to the J-6 as required.

(11) Approves, in conjunction with its Configuration Management Board and prioritizes ECPs and ensures that action is taken to implement approved ECPs, monitor progress, and enforce milestones for completion.

c. Manage the long-haul communications network that supports GCCS connectivity to each site's GCCS premise router. Provide technical assistance for local connectivity requirements. Provide procedures to ensure users without direct access to GCCS through either Wide Area or Local Area networks can access the system.

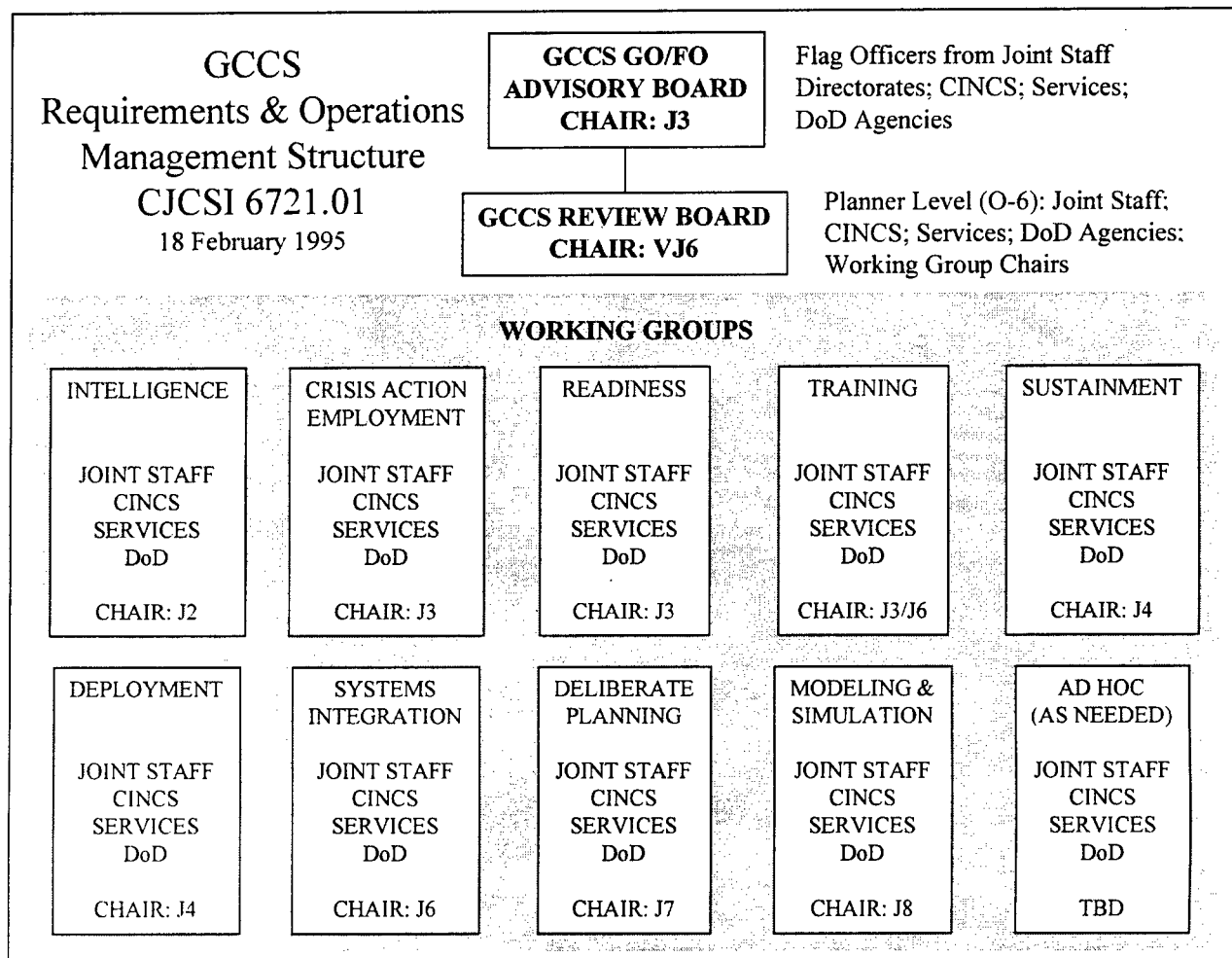
11. Other Defense Agencies

a. Collaborate in the development and implementation of GCC requirements related to their activities as tasked by the appropriate Joint Staff directorate.

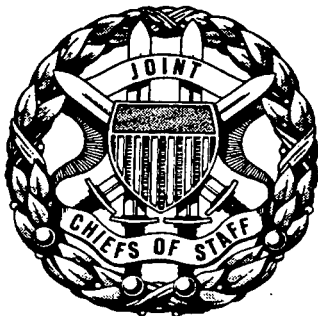
- b. Determine the impact and feasibility (procedural and technical) of GCCS information exchange requirements.
- c. Support the OPR and J-6 by planning, programming, budgeting, and funding GCCS interface requirements and necessary internal initiatives within fiscal constraints.

ENCLOSURE B

GCCS REQUIREMENTS AND OPERATIONS
MANAGEMENT STRUCTURE



Appendix B



CHAIRMAN OF THE JOINT CHIEFS OF STAFF MANUAL

J-3

DISTRIBUTION: A,B,C,J,S

CJCSM 6721.01

15 March 1997

GLOBAL COMMAND AND CONTROL SYSTEM (GCCS) FUNCTIONAL REQUIREMENTS EVALUATION PROCEDURES

References: See Enclosure F.

1. Purpose. This manual describes the process for submitting joint functional requirements for the Global Command and Control System (GCCS). If approved, new joint requirements become GCCS applications. It also defines responsibilities and describes specific coordination procedures to take a requirement through the validation, assessment, and approval process.
2. Cancellation. J-6A 00485-95, 21 April 1995, "Global Command and Control System Functional Requirements Evaluation Procedures," is canceled.
3. Applicability. This manual applies to Combatant and unified commands, Services, Defense Agencies (C/S/A) and the Joint Staff. The procedures in this manual only apply to joint requirements.
4. Procedures. Specific procedures for inputting new joint requirements into the GCCS requirements process are in enclosure C. Enclosure D is a flow chart of the actual process.
5. Additional Copies of This Manual. Joint Staff directorates may obtain a limited number of additional copies of this manual from the Records Management and Automation Support Branch, Room 2B917. The Services, combatant commands, and Defense agencies and all other holders are authorized to reproduce, print, and stock copies of this manual to meet their internal distribution requirements.

6. Effective Date. This manual is effective upon receipt.

// signed //
STEPHEN T. RIPPE
Major General, USA
Vice Director, Joint Staff

Enclosures:

A--General Information
B--Responsibilities
C--New Requirements Approval Process
D--Functional Requirements Procedures Flow Chart
E--GCCS Requirements Database (GRiD)
F--References

DISTRIBUTION

Distribution A, B, C, and J plus the following:

	<u>Copies</u>
President, National Defense University.....	5
Naval War College.....	5
ASD(C3I).....	5

(INTENTIONALLY BLANK)

ENCLOSURE A

GENERAL INFORMATION

1. Background. Global Command and Control System (GCCS) supports users from the NCA through the Joint Task Force through its component commands as well as Service components and Agencies. Joint user requirements are met in GCCS by finding and integrating the best of existing C/S/A systems and other C2 systems or by showing the need to find or make an application or support system in response to a functional user requirement. The key elements of the GCCS requirements process are as follows:

a. Requirements Process Goal. The goal of this process is to provide the smartest, most responsive method of integrating applications best meeting our warfighter's needs at the best dollar value of the life-cycle of the product. The chief consideration is to accurately define what the warfighter needs, find the best solutions government or industry has to offer, and make a decision using select judgment criteria to implement the most cost-effective solution. Necessary to develop smart solutions and integrate new joint requirements is a strong partnership of the program manager, the warfighter-user, and the Global Command and Control (GCC) management structure.

b. Acquisition Methods and Oversight. In accordance with reference f and described in detail in reference d, this requirements process can use innovative practices and new approaches to streamline the acquisition process, reduce infrastructure, and enhance customer service. The process in this manual uses an evolutionary acquisition strategy, under the management and oversight of Integrated Product Teams (IPTs). The resulting IPTs fall under the auspices of the Major Automated Information System Review Council (MAISRC) and ASD(C3I).

c. Requirements Determination. Users must first assess mission needs to determine if they can be satisfied by non materiel solutions such as changes in doctrine, operational concepts, tactics, training, or organization. If users can not satisfy mission needs by nonmaterial solutions, they can try a new requirements definition.

15 March 1997

d. Inputting Joint GCCS Requirements. GCCS users send new joint requirements to the Joint Staff through their appropriate CINC, Service or Agency office of primary responsibility (OPR), or GCCS working group. The description of the requirement including candidate applications is then submitted via the GCCS Requirements Data Base (GRiD) for processing. If a GCCS working group identifies a new requirement, the working group is responsible for inputting the requirement into GRiD and performing initial validation before the Assessment I stage. The GCC management structure validates, assesses, approves, ranks, and selects the best capability to satisfy user requirements for submission into the applicable Evolutionary Phase Implementation Plan (EPIP). The EPIP is a contract to set up a performance baseline among the entire user community, or stakeholders, which includes the Joint Staff, DISA, developers, and C/S/A. The EPIP summarizes how to satisfy requirements and by whom, the associated costs of development, risk of implementation, economic analysis associated with implementation of the GCCS phase, testing of the technical solutions, and the schedule for completing the phase. Also, the EPIP gives developers the opportunity to take advantage of emerging technologies, keeping GCCS functions fresh. Validation of requirements and integration of the resulting applications to GCCS will be consistent with GCCS development and implementation plans approved by the GCC OPR, Joint Staff J-3, in accordance with reference a. At a minimum, requirements should support the GCCS goals in this manual.

e. Service or Agency Specific Requirements. Only joint requirements need to go through the process described in this manual. Services and Agencies are encouraged to have a similar process of working Service or Agency-specific requirements as described in this manual. New requirements should strive to improve these areas:

- 1) Improve the timeliness and accuracy of information to decision makers and the means to send out resulting decisions.
- 2) Enhance and speed the decision cycle to operate within the adversary's decision cycle.
- 3) Improve interoperability among forces (CINCs, components, national organizations, coalition, and allied).

15 March 1997

- 4) Meet the C2 requirements of the NCA and joint command levels down through the Joint Task Force component commanders. Improve the common situation awareness to enhance national and military leaders' ability to perceive, convey, and share ideas and knowledge.
- 5) Supply a fused, real time, true representation of the warrior's battlespace (integrated RED/BLUE/GRAY picture) to establish a dominant battlefield awareness.
- 6) Improve the ability to coordinate, order, and respond vertically and horizontally to the degree necessary to prosecute the mission in the battlespace.
- 7) Improve the mobility and agility of the deployable C2 force.
- 8) Reduce life-cycle costs such as future maintenance or training.
- 9) Improve C2 infrastructure support ability and flexibility in any environment.

f. Application Evaluation. Guidance, evaluation criteria, and various checklists are provided to assist GCC Working Groups and IPTs to evaluate and set priorities on requirements and associated or proposed new applications. After an initial validation, two assessment phases examine the suitability of candidate applications in terms of functional effectiveness, cost to implement and support, and technical feasibility.

g. Application Selection. In the assessment phases, a selection process will occur to select the application or multiple applications that best satisfy any requirement. To find the best fit of application to requirement, working groups or appointed lead elements (see definitions) should search government and commercial sources to find applications that may meet requirements under evaluation. Working groups should make objective and meaningful selection criteria and/or decision tools to select the application best meeting user and joint community requirements. It is important to the requirements process, for working groups to work off the same base of facts. Decisions must be based, at a minimum, on criterion that

15 March 1997

consider the ability to fulfill requirements defined by the customer, cost to implement, and risk analysis. Working groups may choose to modify candidate applications under evaluation to meet other validated requirements in the system as long as customers agree modifications meet all requirements.

h. Configuration Management. New candidate applications must meet all configuration management items developed by the DII COE Configuration Control Board, the GCC management structure, and be at least level 5 DII COE compliant. If a Service-unique application has joint utility, other C/S/A may use this requirements process to possibly adapt or modify the Service application for joint use. The GCC management structure may in-turn appoint the Service as the lead element for implementation. Configuration management will provide the appropriate process to handle configuration control of all source documentation.

i. New Developmental Efforts. A major goal in the initial implementation strategy is to determine if modification of existing applications satisfy requirements to lessen new developmental efforts. Working on new developmental efforts will only be done when they are the most prudent, appropriate, cost-effective, and efficient method to satisfy new requirements.

j. Changes to GCCS. Generally, there are three categories of changes that will prompt a revision to the GCCS operational environment: Many of which may be included in a new run version:

(1) Approval of new joint requirements.

(2) Implementation of Change Requests (CRs) and Problem Reports (PRs) (Note: send PRs and CRs to the DISA GCCS Management Center (GMC)).

(3) Approved technical or functional modifications.

Being able to identify the correct category for a change is important, because each is handled differently in the process. Refer to the Enclosure C and paragraph 2 below for the meaning of each category and how to handle them.

2. Definitions.

15 March 1997

- a. Acquisition Category (ACAT). Categories for acquisition programs are based upon size and complexity. GCCS is designated an ACAT 1M for which the Milestone Decision Authority (MDA) is ASD(C3I). The "M" refers to Major Automated Information Systems Review Council (MAISRC).
- b. Change Requests and Problem Reports. CRs are updates, modifications, or enhancement to existing applications made to meet current requirements. PRs are changes necessary for resolution of existing modules. Such changes normally do not significantly change the GCCS baseline or require an evolutionary build. CRs are normally not generated to fulfill new requirements if they change the baseline of the GCCS data base, are technically difficult, costly, and time consuming.
- c. Common Operational Environment (COE). COE establishes an integrated software infrastructure that facilitates the migration and implementation of functional mission applications and integrated databases across information systems throughout the Defense Information Infrastructure (DII). The DII COE provides architectural principles, guidelines, and methodologies that assist in the development of mission applications software by capitalizing on a through and cohesive set of infrastructure support services. The DII COE architecture is made up of a kernel application that supplies the basic operating system services and two principle components: (1) Common Support Applications, and (2) Infrastructure Services.
- d. Configuration Item (CI). CI is an aggregation of hardware, software, processed materials, services, or any discrete portions designed for configuration management and treated as a single entity for configuration management process.
- e. Configuration Management (CM). CM is a management discipline applied to technical and administrative direction to the development, production, and life-cycle support of a configuration item (CI). The discipline is applicable to hardware, software, processed materials, services, and related technical documentation. The application of CM for GCCS is a method to make changes to the operational GCCS in the field without detriment to the operational state of the baseline.

15 March 1997

f. Commercial-off-the-Shelf (COTS) Applications. COTS applications are purchased from and licensed by their manufacturers. Changes to COTS software baselines, other than those required by the DII COE Integration and Runtime Specification (I&RTS) segmentation process, will consist of vendor version upgrading or problem fixes by the vendor. DISA will be the sole authority responsible for coordinating resolution of CRs or PRs with the COTS products vendor.

g. Defense Information Infrastructure. DII is a DISA and OSD(C3I) approach for building interoperable systems with a collection of segmented software components. It includes a software infrastructure for supporting mission applications and a set of guidelines and standards. The guidelines and standards specify how to integrate existing software and how to properly build new software to make integration seamless and, if at all possible, automated. During the assessment phases, new GCCS requirements will receive a rating of one of eight levels of DII COE compliance.

h. Evolutionary Acquisition Strategy. This strategy is a streamlined, flexible, and evolutionary acquisition framework using an acquisition strategy under the management and oversight of an IPT. This process takes advantage of emerging technology to enhance functionality. The evolutionary approach is characterized by the design, development, and deployment of a preliminary capability using current technology. This approach includes provisions for the evolutionary addition of future capabilities as requirements are further defined and technologies mature. This strategy maximizes the use of proven state-of-the-art technology.

i. Evolutionary Phase Implementation Plan (EPIP). EPIP is a contract with the customers, OSD, DISA, and Joint Staff as stakeholders, which identifies cost, performance, schedule, test, risk, and budgetary information for implementation of new requirements. The EPIP is specific in nature and provides a plan, which identifies all necessary criteria for successful completion of a particular implementation phase. EPIPs are phased actions geared toward meeting the requirements outlined in the Requirements Implementation Document (RID).

j. Integrated Product Team. The Secretary of Defense has directed the Department of Defense to perform as many acquisition functions as possible, including oversight and review, using IPTs. IPTs will

15 March 1997

function in a spirit of teamwork with participants empowered and authorized, to the maximum extent possible, to make commitments for the organization or the functional area they represent. IPTs consist of representatives from all appropriate functional disciplines working together to build successful programs and enabling decision-makers to make the right decisions at the right time. Reference d contains specific procedures on how IPTs operate. The three types of IPTs are:

(1) Overarching IPTs (OIPTs). OIPTs focus on strategic guidance, program assessment, and issue resolution. The OIPT is chaired by ASD (C3I). The OIPT is the decision making body and approval authority for the RID and EPIP.

(2) Working Level IPTs (WIPTs). WIPTs find and resolve program issues, determine program status, and seek opportunities for acquisition reform.

(3) Program IPTs. Program IPTs focus on program execution, and may include representatives from both government, and after contract award, industry.

IPTs are an integral part of the defense acquisition oversight and review process. For programs designated as ACAT IAM, such as GCCS, there are generally two levels of IPTs: OIPTs and WIPTs. For each program, there will be an OIPT and at least one WIPT. WIPTs focus on a particular topics such as cost, performance, risk analysis, test, and economic analysis.

k. GCCS Application. Any software module or modules that provide functionality to fulfill a GCCS requirement.

l. GCCS Approval Authorities. The responsible authority in each C/S/A that can submit new requirements into GRiD. Each C/S/A appoints an approval authority to validate and approve new GCCS requirements for submission into GRID. Each organization may delegate this function as needed—approval authorities must be at least the O-6 level. The preferred method is to appoint one section in each C/S/A to act as a clearing house in submitting joint requirements.

15 March 1997

- m. GCCS Joint Requirement. A joint requirement demands a change to the GCCS baseline or starts a new evolutionary build. New joint requirements are submitted to J-33/CSOD through the GRiD described in Enclosure E and according to the procedures in this manual.
- n. Government off-the-Shelf (GOTS) Applications. GOTS are government owned and developed applications.
- o. Lead Element. A CINC, Service, or Agency designated the responsibilities by a GCCS working group to carry out assessment or other assigned functions.
- p. Migration. Migration is a process of making an application DII COE compliant.
- q. Major Automated Information System Acquisition Program Review Council (MAISRC). MAISRC is the senior DoD automated information systems acquisition review board chaired by ASD(C3I). MAISRC advises ASD(C3I) on major decisions on individual automated information system programs, specifically, and AIS acquisition policies and procedures.
- r. Modification of Existing Requirement or Technical Implementation. A modification to an existing requirement is a change in functionality, which may require more than minor alterations to an application. Modifications are different from CRs because of the technical difficulty of implementation, associated funding, and possible impact on other functions. Modifications require an assessment from the GCC management structure to determine the best implementation.
- s. Requirements Implementation Document. RID is a living document providing broad overarching requirements for GCCS. It describes future warfighter requirements validated and ranked by the Joint Staff, J-3, and agreed to by the stakeholders. The approval authority for the RID is ASD(C3I). To complete objectives in the RID, many phases or EPIP documents may be necessary.
- t. Users. Users are any organization or individual that uses GCCS to oversee, conduct, and support C2 activities. In the context of this manual, principal users are the NCA, C/S/A, and the Joint Staff. User participation in requirements definition, throughout evaluation,

CJCSM 6721.01
15 March 1997

development, and fielding of applications, is critical to the successful implementation of GCCS requirements.

CJCSM 6721.01
15 March 1997

(INTENTIONALLY BLANK)

ENCLOSURE B

RESPONSIBILITIES

1. GCCS Functional Requirements Responsibilities. This manual identifies responsibilities regarding the definition, submission, validation, assessment, prioritization, funding, and development of new GCCS requirements. The GCCS management structure including specific management responsibilities as it pertains to GCCS can be found in reference a.

a. Requirements Submission. All C/S/A and GCCS working groups may input requirements for GCCS. The submission must be endorsed at the O-6 level (GCCS Review Board Member or Working Group Chair) or above, to the Joint Staff, J-33/Command Systems Operations Division (CSOD). The preferred method is to establish an approval authority as the OPR in each C/S/A to act as a clearing house for joint GCCS requirements submission. Once approved for submission, it must be entered into GRiD to start the requirements process. Management reports in the GRiD will be used to keep the cycle time for the requirements process down. Information on GRiD and how to input requests is at Enclosure E.

b. Funding. Funding responsibilities are according to the guidance contained in reference b.

(1) Services and agencies supporting GCCS will establish GCCS program management offices (PMOs) to implement GCCS. The PMOs will manage all Service and agency-sponsored commands and organizations including support to combatant commands and combined joint task force commands to the lowest level requiring GCCS capabilities. GCCS PMOs within the Services and agencies will meet on a periodic basis and report efforts to ASD(C3I).

(2) Each Service will consolidate all funding in support of GCCS to the Service GCCS Program Element (PE). The PEs will include all resources required to support life-cycle management of the GCCS to include all appropriations necessary for the continued support and evolution of GCCS. The PE will include all resources assigned to life-cycle support of Defense agency-sponsored C2 programs, that support GCCS and the former WWMCCS ADP programs.

15 March 1997

(3) DISA will program funds for implementation of its responsibilities within the DISA GCCS spending plan. DISA is responsible for systems management life-cycle support of Joint applications, assessment of CINC and Service applications, architectural and standards definitions, management of the COE, data standards, configuration control, systems engineering, interoperability testing, software testing, and release. DISA has the responsibility to ensure the certification and compliance of Service and agency systems to GCCS standards, to build joint GCCS applications.

(4) Service and CINC requests for GCCS upgrades or replacements to any Service-unique C2 requirements will be assigned to the corresponding MILDEP. Joint Staff and CINC sponsored changes will be assigned to a lead MILDEP by ASD(C3I).

(5) Organizations selected as executive agencies to field applications on GCCS must program funds for operations, maintenance, and modification of the applications. Funding from Services and Defense Agencies (other than DISA) is not controlled by the GCC management structure. Normally CINCs will not be assigned the role as an executive agent.

(6) Organizations nominating applications to GCCS must ensure compliance with applicable Service acquisition and operations activities consistent with Title 10, United States Code, Armed Forces responsibilities.

c. OPR Responsibilities. The J-3 executive agent for GCCS is J-33/CSOD. That office is responsible for the oversight of the requirements process. J-33 will:

(1) Review the requirements data base weekly ensuring all new requirements are assigned to an appropriate working group.

(2) Consolidate and aggregate like requirements entered into the GRiD for action by the appropriate working group.

(3) Advise the chair of the GCC Review Board for possible formation of an ad-hoc working group for requirements not fitting into one of the existing working groups.

(4) Provide quarterly reports via GRiD to the Chair of the GCC Review Board and other working group chairpersons on new requirements and forward them to the appropriate working group chairperson for action.

(5) Track the status of all requirements from identification through fielding and advise users quarterly of the status of all requirements submissions via GRiD. The tracking system must be integrated with the master configuration management data base maintained by DISA.

(6) Provide an update on status of migration, modification, and development efforts for each GCCS Review Board meeting.

(7) Provide final resolution on coordinated requirements within the GCCS OIPT.

d. Customer Involvement and Responsibilities. Organizations submitting requirements must provide a point of contact (POC) who can participate through the validation and assessment process. POC's or requesting organizations must:

(1) Focus the requirements definition on the needed warfighter capability. Ensure requirements definitions are complete and accurate.

(2) Monitor the assessment process ensuring the final validated requirement satisfies user requirements as the function migrates into GCCS.

(3) Submit any information on known applications satisfying the requirement. If known COTS, GOTS, or other existing applications in other CINCs or Services best satisfy the requirement, recommend one of those. Applications must meet current DII COE compliance standards for consideration.

(4) Budget funds for travel to participate in the validation process.

(5) Provide functional expertise on functions not familiar to GCC working groups.

(6) Coordinate with the GCCS Operational Testing Authority (OTA) to define testable criteria associated with the requirement.

e. GCC Working Group Responsibilities. Various GCC working groups exist as part of the GCCS management structure as either functional or ad hoc. Each working group has an Assigned Working Group Chair (AWGC) or is co-chaired. Each AWGC or co-chaired will:

- (1) Input new requirements upon appropriate definition into GRiD.
- (2) Establish liaison with other working groups that may have an overlapping interest in the requirement.
- (3) Update status changes to GRiD as they occur.
- (4) Advise other interested working groups of the progress and schedule of validation efforts.
- (5) Coordinate with CINCs, Services, GCCS OTA, and other agencies as necessary during the validation process.
- (6) Convene their respective working groups to recommend validation of requirements submitted for GCCS.
- (7) Perform a search for existing COTS, GOTS, or other applications, which may better satisfy a requirement under consideration. Develop criteria, that selects the best application among a group of possible candidates for integration into GCCS.
- (8) Determine if the requirement or proposed enhancement is valid by using the criteria in Enclosure A and by asking the community most affected by the requirement for inputs. Working groups may choose to have the originator of the requirement demonstrate the utility of proposed applications to the warfighter.
- (9) Inform the chair of the GCC Review Board and J-33/CSOD of requirements or enhancements, that are not valid or need clarification.
- (10) Input valid requirements to the GCC Review Board for signature.

(11) Coordinate with the GCCS OTA and customers to establish valid testing schemes for Operational Testing and Evaluation (OT&E).

f. Systems Integration Working Group (SIWG). The SIWG is responsible for all areas and issues relating to C4 systems integration. The SIWG coordinates its oversight efforts with the GCCS Project manager (PM) to avoid duplication of effort, focusing its work on providing GCCS development requirements to the GCCS PM as outlined in reference a. DISA provides the GCCS PM. In addition to the oversight responsibilities of C4 systems integration the SIWG will:

(1) Monitor the requirements process for requirements that require a technical modification to an existing application that may not be assigned to a functional working group. Technical assessment and cost analysis for requirements such as these will be the responsibility of DISA. Functional assessment will be assigned to a lead element or the submitter of the requirement.

(2) Monitor Advanced Concept Technology Demonstrations (ACTDs) and Leading Edge Services (LES) that enter into the GCCS requirements process.

g. Review Board Responsibilities. The GCC Review Board, as defined in reference a, is the final step in the validation process. The GCC Review Board will:

(1) Approve by signature validated requirements recommended for approval by working groups and the review board.

(2) Coordinate with the appropriate Joint Staff directorates concerning requirements which the GCC Review Board determines are not valid or need clarification. If necessary, return the submission to the sponsoring organization requesting further clarification.

(3) Return submissions to the sponsoring organizations the Joint Staff and GCC Review Board determine not valid for inclusion into GCCS, explaining the reasons why.

(4) Update GRiD as necessary for requirements approval.

(5) Establish a prioritized ranking of all requirements and update the list with each new approved requirement.

(a) Establishing Final Priorities. The GCC Review Board will use all previous recommendations of priorities as a starting point for developing a priority implementation list.

(b) Criteria for Determining Priorities. Using funding information, C/S/A inputs, recommended technical implementation, risk analysis, and other criteria as needed, the GCC Review Board will make a rank order list of candidate applications for implementation into GCCS. The preferred method is to use quantitative decision tools, such as matrices, or any other decision tool at the discretion of the working group chair to make a logical fact-based rank order list. This list will provide key information for the development of the next GCCS EPIP.

(c) Annual Review. The GCC Review Board will annually audit the priority list ensuring items low in the list are not overcome by technology or mission changes.

h. Executive Agents. Executive agents are responsible for developing and maintaining GCCS CIs. They will establish internal GCCS requirements validation, approval, and CM processes consistent with CM policies. They will fund for the operations, maintenance, and modification of applications chosen for inclusion into GCCS. Once an application integrates into GCCS funding responsibility falls back to each the respective Services PE as outlined in Enclosure B paragraph 1.b.(2).

i. GCCS Centralized Management Responsibilities. DISA is responsible for centralized migration management of joint applications for GCCS. DISA will:

(1) Perform technical assessments of all new requirements under evaluation in the review process. This assessment will include an analysis of the testing of technical solutions and the feasibility of implementing technical solutions.

(2) Provide cost benefit analysis of technical solutions, recommend the best technical solutions for overall GCCS implementation, and

15 March 1997

provide input to the GCCS review board on prioritization of requirements and associated technical solutions.

(3) Provide alternative solutions and recommendation of known applications for requirements under evaluation, which may satisfy the requirement better, be more cost effective, or more feasible to implement.

(4) Provide management of the EPIP process. Together, with J-33/CSOD, provide appropriate coordination with ASD(C3I) for acquisition-related issues.

s. implementation of GCCS requirements.

(INTENTIONALLY BLANK)

ENCLOSURE C

NEW REQUIREMENTS APPROVAL PROCESS

1. General.

a. Acquisition Oversight. Acquisition oversight for the GCCS program resides with the ASD(C3I) as detailed in references e and f. The oversight process is a streamlined approach allowing joint requirements definition to go on in an evolutionary fashion. As GCCS progresses, the program will move toward a more streamlined MAISRC process with IPTs working major issues.

b. Streamlined Acquisition Process. The design of the GCCS functional requirements process takes full advantage of the rapid change in technology and the streamlined MAISRC process and keeps pace with the ever changing and expanding mission requirements. This design is a result of an Evolutionary Acquisition Strategy (EAS). EAS provides flexibility and responsiveness by integrating an infrastructure of area experts to provide swift and agile assessment, validation, and fielding of new requirements. This process consists of several phases, which new requirements can access at different levels depending upon the priority, risk, or level of difficulty of change. The phases are; Requirements Definition, Validation, Assessment I, Prioritization, Assessment II, and Development (which includes Operational Test and Evaluation and Fielding). To enhance this entire process, customers are encouraged to field test new requirements, suggest COTS or GOTS software, or provide suggestions for technical solutions. However, requirements submission must include a good description of the required function addressed in terms of mission need or capability rather than merely citing hardware or software technical solutions.

2. Requirements Definition. This is one of the most important phases and is key to review and validation of the requirement. The scale of new requirements range from completely new functions requiring full-scale development or acquisition to modifications or enhancements to existing functions. Some modifications or enhancements may fall into the realm of CM and will follow the processes that will be outlined in CM policy. PRs and CRs need to be worked through the DISA GCCS Management Center (GMC), they are generally not new requirements.

15 March 1997

PRs address problems with existing functions that do not meet requirements for whatever reason for which they were designed. CRs address changes to existing functions to enhance or provide additional capability. For CRs that arise that provide new functionality, may satisfy any part of a new requirement, and are significantly costly in technical and monetary terms, DISA and the Joint Staff will decide jointly how best to handle the CR. New requirement submissions should meet the intent of GCCS program goals and address mission needs or capabilities. The following checklist contains key elements to include in any new requirements submission and must be a part of the submission. Include these elements in the detailed description field of the GRiD program outlined in Enclosure E.

- a. Describe and define the deficiency with respect to mission performance.
- b. Describe the requirement in terms of functional capability.
- c. Define the possible customer base that could or would use the new function.
- d. If applicable, identify requirement as either location specific, coalition or combined.
- e. List possible interfaces with other GCCS functions.
- f. Exit criteria. Describe the new capabilities that will result upon implementation.
- g. Name appropriate performance standards, associated measures, and minimum acceptable threshold levels of the resulting application.
- h. Integration environment. Name any unique application required to perform the mission. Justify why existing similar systems do not satisfy requirement.
- i. If the requirement is a modification to an existing system, ensure migration will be DII COE compliant. Provide the level of DII COE compliance.
- j. Required interfaces beyond GCCS.

15 March 1997

k. If the requirement will result in a Service-specific or site unique application to become a joint application, provide the specifics of the application's functions relative to the new joint requirement. Also, if available, cite source documents that may exist that provide reasons for this application to be a joint application.

l. Determining Priority. The next step is to determine the operational priority of the requirement. Use the following categories to determine priorities for new joint requirements submission:

(1) Category 1. Mission critical requirement essential to readiness, has a direct impact on warfighting capability. Requirement is proximate: needed immediately. Requirements are driven by the JSCP or are found in the CINC's Integrated Priority List (IPL), noted in the CINC's Preparedness Assessment Reports (CSPARS), or the CINC's Critical Item List (CIL).

(a) 1.A. The present function does not exist on GCCS.

(b) 1.B. The present function partially exists but all or most of the key elements of the new requirement are not satisfied.

(c) 1.C. The present function exists but at least one key element of the new requirement is not satisfied..

(2) Category 2. Mission essential requirement, indispensable for maintaining sufficient military capability for mission performance. Requirement is pressing: needed no later than a future specified date. Some requirements that may be found in the POMs, tied to a Joint Strategic Review (JSR) issue paper, or top priority in the Joint Planning Document.

(a) 2.A. The present function does not exist on GCCS.

(b) 2.B. The present function partially exists but all or most of the key elements of the new requirement are not satisfied.

(c) 2.C. The present function exists but at least one key element of the new requirement is not satisfied..

(3) Category 3. Significant enhancement. Necessary requirement to keep step with master plans, migrations, and POM initiatives. New requirement will represent a significant increase in mission capability or command and control.

(a) 3.A. The present function does not exist on GCCS.

(b) 3.B. The present function partially exists but all or most of the key elements of the new requirement are not satisfied.

(c) 3.C. The present function exists but at least one key element of the new requirement is not satisfied..

k. Technical Change Categories. The final step of requirements definition is to determine the type of technical change necessary to achieve the requirement. This determination must parallel the priority category determination of existing functions on GCCS. Select one of the categories below and provide supporting information as to why the respective technical change applies in the Detailed Description field of GRiD outlined in Enclosure E. There are generally four types of technical changes that will determine which phase of the process the requirement will start.

(1) New Requirement No Precedent. In this case the requirement is a totally new requirement—there are no existing applications on GCCS that can perform the necessary functions. The requirement will require totally new software or functions. This is a new requirement that will start with validation, but will require a good description of the required function(s) or capabilities.

(2) Modification of Existing Function. In this case an existing function can be modified to perform the new requirement. To fall into this classification a major change in the existing software or data bases will effect a change in the GCCS baseline. This requirement will enter Assessment I phase. This case will require a technical and cost analysis from DISA before proceeding to prioritization.

(3) Modification of Technical Implementation. In this case existing COTS, GOTS, or minor software changes, that alter the GCCS baseline satisfy the requirement. This may be a requirement that was successfully tested in a Joint Warfighting

15 March 1997

Capabilities Assessment (JWCA) or an Advanced Concept Technology Demonstration (ACTD) with a C/S/A sponsor and shows great promise. In many cases some of these functions may already be field tested, by the customer and this represents final validation and approval for the entire system. This requirement can be evaluated, tested and implemented easily and may preclude prioritization. This requirement will enter a shortened Assessment I phase in which DISA in conjunction with a lead element or working group, will quickly review requirements, costs, technical feasibility, and CM.

(4) Hardware or Software Upgradings. In this final case, necessary hardware and software changes to existing GCCS elements are needed to enhance or provide new functionality. This excludes CRs and PRs. In some cases the next version of COTS or GOTS software provide enhancements necessary to provide increased capability. Some enhancements could be upgrading hardware to increase speed or capacity. This requirement will be scheduled for development and fielding. This type of change will demand a change to the existing GCCS baseline.

3. Validation. The validation phase confirms requirements definition is complete, the priority assigned in GRiD by the user is correctly applied, and initial technical evaluation assigned by the customer is correct. This initial validation is really a confirmation that the requirement is ready to begin the process. This step is the responsibility of the J-33/CSOD or the respective working group, if the requirement is submitted by a working group. If the requirement submission did not come from a working group, depending upon the functionality of the requirement, CSOD may assign the requirement to an existing or ad-hoc working group if necessary. The working groups will then perform an initial review and assessment of the requirement.

(a) Assignment of an Executive Agent or Lead Element.

Throughout the requirements process, but as early as validation, working groups may assign an executive agent or lead element to perform some or all of the functions of assessment, testing, and development as necessary. Lead element responsibilities usually will entail searching, evaluating, and testing of candidate applications, or lead development actions of technical solutions. Executive agents will normally perform more actions than a lead element, including development of technical solutions, technical

analysis, and on-line performance testing. The decision to assign executive agent responsibility to a Service may have to be made at the GCC review board level. Executive agents or lead elements will work under the supervision of working groups and perform functions tailored to the situation. For instance, a Service element may take on the role of an executive agent or lead element when requesting a Service-unique application be made a joint application.

(b) Exit Criteria for Validation. To move on to Assessment 1, the following must be complete:

- (1) Requirements definition is complete.
- (2) The priority is correctly applied.
- (3) Initial technical evaluation is complete and correct.
- (4) Assignment to a working group.

3. Assessment I. This phase is a quick verification that certain conditions exist in order to warrant more serious analysis and assessment. Also, in this phase a preliminary technical solution is made. In this stage, GCCS working groups:

- a. Determine the extent to which existing applications provide the necessary functions of the new requirement.
- b. Verify the customer applied the correct priority criteria.
- c. Identify CRs and PRs mistakenly submitted as requirements and route them to DISA for action.
- d. Solicit other C/S/A for similar new requirements to compare with for selection of the best technical solution or application for implementation.
- e. Route the requirement to the following organizations or teams for each respective function listed:
 - (1) DISA for analysis of the feasibility of development and initial determination of the OT&E strategy. For smaller, well-developed COTS and GOTS applications, perform initial testing if practical.

15 March 1997

(a) Early testing may be appropriate at this time if applications on hand look promising, time and costs permit, and there is an urgency to fill the requirement. The fundamental purpose of test and evaluation (T&E) in this stage is to show the areas of risk to be reduced or cut early in the process.

(b) Assessment I early testing is conducted to demonstrate the feasibility of conceptual approaches, evaluate design risk, find design alternatives, compare and analyze trade offs, and estimate satisfaction of operational requirements.

(2) DISA for Configuration management in accordance with current CM policy.

(3) Appropriate IPTs for preliminary cost, schedule, economic analysis and other issues as necessary. For example the Risk Working-level IPT (RWIPT) will provide a quick risk analysis (an in-depth analysis will occur in Assess II if necessary). Final outcome of WIPTs work, in conjunction with DISA, will provide a risk profile of either low, medium, or high for implementation that considers:

(a) Cost of implementation and affordability.

(b) Degree of difficulty of change to GCCS baseline.

(c) Timelines of implementation.

(d) Technical feasibility of implementation.

(e) Comparison of all resource expenditures versus expected mission payoff.

(f) Life-cycle support and affordability.

(4) RWIPT for risk analysis. In conducting risk analysis a decision matrix is an effective methodology for managing program risks and is a good tool for streamlining the process. The matrix can serve to quickly focus the team on selecting a specific set of evaluation criteria to address the program risks. The final result combined with the priority assigned by the customer will become

key decision elements in determining priority. Teams working risk analysis should use decision matrices or another fact-based decision tool as a primary method to conduct analysis and provide a risk profile.

7. Exit Criteria for Assessment I. The final outcome of Assessment I is a preliminary technical solution, a simple risk profile that includes verification that the technical solution is or can be made DII COE compliant, is cost effective to implement, is economically and technically feasible and can be implemented in a reasonable time. The assigned working group in conjunction with the originator of the requirement makes the decision that all elements of Assessment I are complete.

8. Prioritize Requirements. In this phase working groups provide the GCC Review Board priority recommendations of new requirements. In making ranking recommendations working groups will use the risk profile as one of the major factors of consideration. The validated customer-assigned priority should provide a good starting point for this process. To move on to Assessment II, the application of the associated requirement must high enough in the prioritization list to warrant integration into GCCS.

9. Assessment II. This phase is a detailed shakedown of the candidate application or proposed technical solution with the assumption that it is headed for final development. In other words, the technical solutions, are technically and economically feasible to implement at this time and will provide the warfighter the necessary functions described in the requirements. In this phase, DISA, Joint Staff J-6, and any lead elements or executive agents will confirm architectural direction, select system hardware and software design, and build and test the architecture. DISA will determine architecture requirements before designing. The preferred method is on-line testing in an active environment by one Service or Agency. Use of real data will provide the best possible test of the new application. If all or part of the new application does not exist for testing but needs full scale development, the assessment may begin with testing of a mock-up configuration. Two other actions will occur during the Assessment II phase:

- a. Operational Testing and Evaluation (OT&E). The degree of OT&E of each new requirement is determined by the associated level of risk and the degree of compliance of the application under assessment. Assessment II should provide all the information necessary to

15 March 1997

develop a detailed risk analysis and degree of compliance of the candidate application. If more information is needed before testing, DISA will work with the appropriate IPT to complete the necessary study. Consideration should be given to combining developmental testing (DT) and operational testing (OT) to streamline the process.

b. Training. A training concept of operations (CONOPs) is prepared in Assessment II with heavy consideration given to providing some training during DT and OT.

10. Exit Criteria for Assessment II. The final outcome of Assessment II is a staffed and approved EPIP.

11. Development. This phase includes resolving any user design issues and developing the technical detailed design for each application. Once the design is complete, either DISA or an appointed lead Service or agency will produce user procedures and training materials, plan and implement any final system testing, and file conversions. Upon development the system is prepared for implementation and system performance measures are applied ensuring the application meets customer requirements. Implementation may include integration of existing GOTS or COTS software into GCCS and preparation of the environment (space, power, etc.) to ensure it is fully ready for the new system operation.

CJCSM 6721.01
15 March 1997

(INTENTIONALLY BLANK)

APPENDIX A TO ENCLOSURE C

SELECTION OF THE BEST FIT APPLICATION

1. Selection Process. To ensure only the best possible known applications reside on GCCS, working groups will use a selection process that strives to select leading applications or technical solutions to fill requirements. Working groups may assign a lead element or executive agent to work the actual process. The lead element could be the customer, a Service component, a panel of the working group, or any other appropriate agency that can best perform the process tailored to the requirement. A validated requirement should lead to the search of candidate applications or technical solutions best meeting the requirement. Even if the requirement's sponsor provided a candidate application, a search should take place to ensure there are no other applications, that might better fill the requirement in terms of functionality, cost, time to deliver, and ability to support. In striving for the goal of C4I For the Warrior, working groups will coordinate with other Department of Defense organizations, where possible, to reduce and eventually eliminate duplication of effort, stovepiped systems, and conflicting standards. The final recommendation of the best fit to the GCC Review Board is determined by the stakeholders.

2. Goal of the Selection Process. The goal of the selection process is to make the smartest, most responsive selection of the best goods meeting the warfighter's needs, at the best dollar value of the life-cycle of the product. In short, find the best fit of an application to fill the needs of the warfighter.

3. Selection Criteria. All candidate applications must be DII COE compliant to the current acceptable level before integration into GCCS. Each requirement will have its own unique parameters, which will drive the selection process. Along with the requirement's parameters, key selection criteria should include at least these factors:

- (a) Implementation factors of cost, technical feasibility, and, time.
- (b) Utility to the joint community.
- (c) Perceived endurance of the application (e.g., will this application last a long time or need frequent updates?).

- (d) Flexibility of the application.
- (e) Ease of use (is it intuitive or will it require extensive training?).
- (f) Compatibility with other applications (is it stand-alone, or can outputs be used in other applications?).
- (g) Scaleability.
- (h) Supportability.

4) Searching for the Best. The cycle time on requirements submission to approval needs to be as short as possible to make GCCS a viable system. Therefore, searches for possible candidates need not be exhaustive, but sufficient enough to ensure not to overlook more cost-effective and robust applications. The best-fit search process and cycle time should be tailored to the urgency and importance of the requirement. Also, to ensure broad and robust GCCS evolution and prevent parallel development of similar applications, searches need to occur across the Department of Defense (DOD). Working groups should ask for inputs for candidate applications for new requirements across the user community. In addition to the user community, working groups or lead elements can search for possible candidates from these sources:

- (a) Organizations such as Defense Advanced Research Projects Agency (DARPA) or any federally funded research organization.
- (b) Government software development agencies.
- (c) Advanced Concept Technology Demonstrations (ACTDs). ACTDs provide the opportunity to streamline the development process. The ACTD process permits early and inexpensive evaluation of mature advanced technology to meet the needs of the warfighter. Working groups must ensure, however, when using ACTDs as a source that the requirement drives the process and not the technology. If an ACTD looks promising, it may be appropriate to encourage the customer to sign up as the sponsor if the program does not already have one. CINCs may act as the sponsor of an ACTD project. The ACTD program usually will leave up to 2 years worth of additional funding after program acceptance, before that funding runs out the Service Program Elements will need to begin the POM process for life-cycle support. The entry point for ACTDs is the GRiD, providing there

15 March 1997

is a sponsor for the ACTD. The Systems Integration Working Group (SIWG) will assist J-33 CSOD in assigning a functional working group the task of taking the ACTD through the GCCS requirements process. The SIWG will monitor the progress of the requirements process to ensure that the ACTD process and the GCCS requirements process are cohesive and that assessment information is shared.

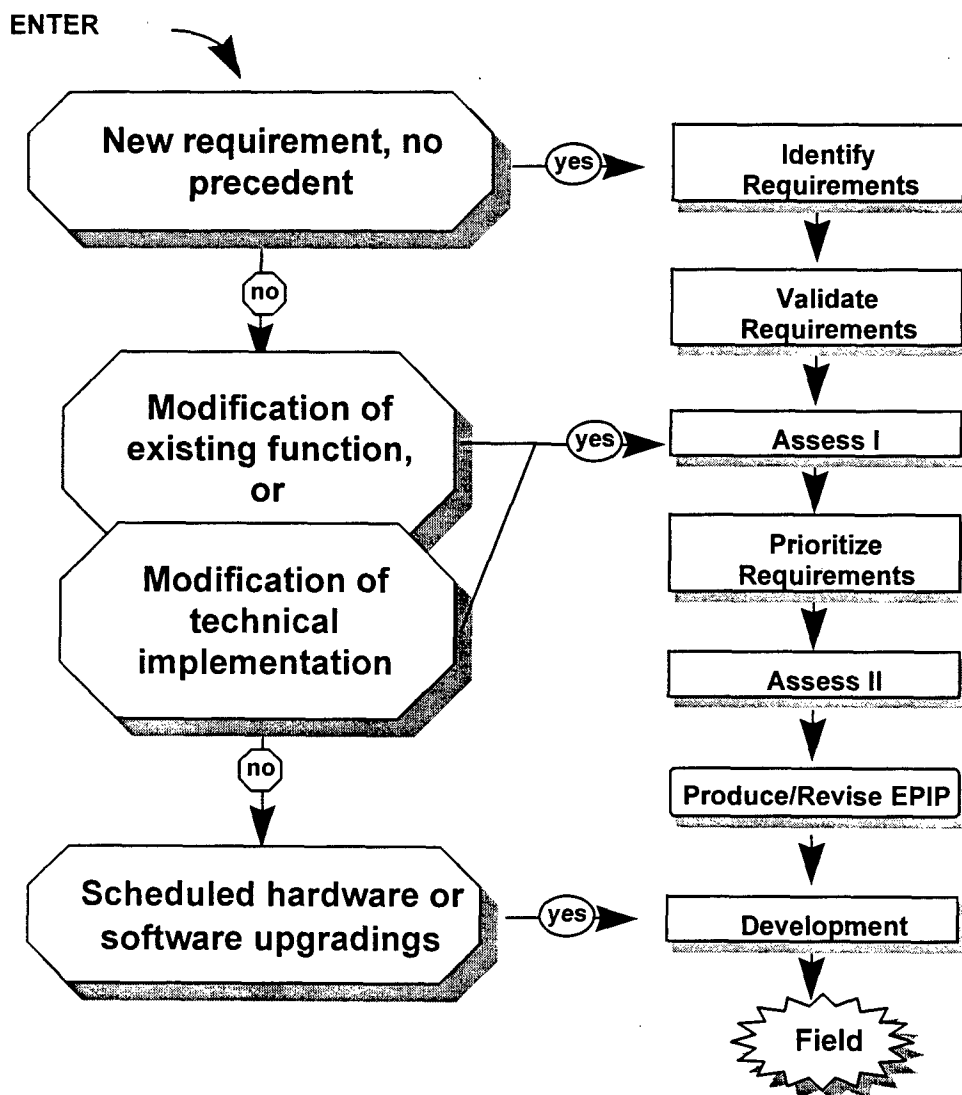
(d) Commercial software firms. Commercial software can provide a wealth of functionality, however, care must be taken to ensure that the software is DII COE compliant to the appropriate level, that future mission changes won't result in expensive modifications to the applications, and that proprietary laws (e.g., exercise caution with COTs products that use proprietary protocols embedded in the software) are closely followed. It may be appropriate to engage legal checks on commercial software licensing early in the process.

(INTENTIONALLY BLANK)

ENCLOSURE D

FUNCTIONAL REQUIREMENTS PROCESS FLOW CHART

1. The GCCS requirements process shown here was taken from reference c. This flow chart shows a graphic representation of the process GCCS requirements follow from identification to fielding.



(INTENTIONALLY BLANK)

ENCLOSURE E

GCCS REQUIREMENTS DATA BASE (GRiD)

1. General. GRiD is a data base management system supporting the submission, validation, and oversight of GCCS functional requirements. GRiD is an application on the SECRET internet protocol (SIPRNET) accessed through the NMCC GCCS homepage on a GCCS workstation. GRiD allows several functions that do not require a User ID or a Login ID: input new requirements, open saved requirements, search database, and management reports. Staffing and most management functions are only accessible to GCCS working groups, J-33 CSOD, or system administrators. J-33 CSOD will manage the GRiD database, fusing like requirements together and combining them into more broader categories for action.

2. Approval Procedures. Generally, inputs into GRiD can only come from established approval authorities from each working group or C/S/A. Each C/S/A will need to appoint an approval authority to handle inputs into the GRiD at the planner level. While anyone may use GRiD to draft requirements, only established approval authorities may submit the request to begin the process. Report the name or names of the GRiD approval authorities for each C/S/A to J-33 CSOD for assignment of a password for access to special GRiD functions. Once requirements finish all steps in the GCCS requirements process, and are recommended for approval by the review board, the recommendations are briefed to the GCC Advisory Board for inclusion into the most appropriate EPIP. The EPIP is the implementation vehicle for all requirements into GCCS. Once an EPIP is built and fully coordinated it is sent to ASD(C3I) for approval and signature.

3. Input New Requirement. Before inputting a new requirement, ensure all necessary information is on hand to complete the request if at all possible. The more complete the information, the quicker validation can begin. While GRiD allows for saving of incomplete requirements, they can not be worked until all required information is put into the data base. The following information is required information on mandatory fields, that must be complete before validation of requirements can begin:

- a. Command or organization.
- b. First name.

- c. Last name.
- d. Address.
- e. Title or name.
- f. Functional name.
- g. Short description.
- h. Detailed description.

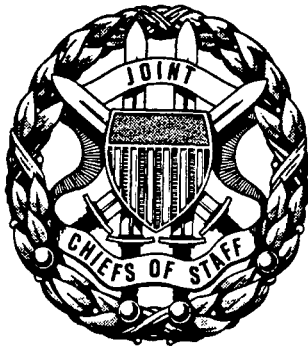
Entering Information. GRiD provides prompts making data entry easy. However, there are a few areas, if defined up front, that will ease the process. Other than assigning a priority as defined in Enclosure C, determining the functional area is critical to the assignment of a working group for assessment. Selecting the field "Functional Area" in GRiD will provide the most current list of functional areas corresponding to working groups. If no functional area applies, select the field "other" and provide a suggested functional area in the detailed description.

ENCLOSURE F

REFERENCES

- a. CJCSI 6721.01 Series, "Global Command and Control Management Structure".
- b. ASD(C3I) memorandum, 26 Jun 95, "Management and Life-Cycle Support for the Global Command and Control System".
- c. Document: GCCS OIPT Briefing by J-33 CSOD 96 to ASD(C3I), 17 Sep 96, "GCCS Evolutionary Acquisition Strategy".
- d. ASD(C3I) Document, Nov 95: "Rules of the Road, A Guide for Leading Successful Integrated Product Teams.
- e. DODD 5000.1 15 March 1996, "Defense Acquisition."
- f. DODD 5000.2-R, 1996, "Mandatory Procedures for Major Defense Acquisition Programs and Major Automated Information Systems".

Appendix C
GCCS Security Policy



CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J6V
DISTRIBUTION:A, B, C, J

CJCSI 6731.01
undated

Reference(s): See Enclosure E

1. Purpose. This instruction identifies and defines the security policy for the Global Command and Control System (GCCS) and GCCS-TOP SECRET (GCCS(T)) and implements DOD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)."
2. Cancellation. None.
3. Applicability. This instruction applies to the Joint Staff, Services, Defense agencies, and unified commands who use, or plan to use, the GCCS.
4. Policy. This policy instruction identifies system characteristics, role responsibilities, the minimum security policy for the system and supporting network, and the minimum security requirements for the GCCS. The requirements are derived from national security policy and an analysis of the operational mission and requirements of the GCCS. Users may process up to SECRET information on GCCS, or TOP SECRET information in the case of GCCS(T). The policy includes a system classification statement, the minimum system security requirements, and the network security policy. All references in this instruction to GCCS include both GCCS SECRET and GCCS(T)

applications and procedures unless otherwise specified. A separate procedures manual, CJCSM 6731.01 will provide the procedures, equipment configurations, and methods to ensure that the GCCS meets the minimum security requirements.

5. Definitions. See the Glossary.

6. Responsibilities.

a. The Chairman of the Joint Chiefs of Staff is responsible for:

(1) Developing a GCCS Security Policy that supports user requirements and selected solutions. This policy will be consistent with DOD information security policy, automated information security policy, and defensive information warfare policy, strategy, and doctrine.

(2) Identifying the minimum system security requirements for GCCS system developers.

(3) Identifying conditions or requirements for entry to various program phases. These phases include, but are not limited to: operational test (OT), initial operational capability (IOC), full operational capability (FOC) and system shutdown/termination.

b. The Director for Command, Control, Communications, and Computers (J-6), Joint Staff, supports the Chairman and J-3 in accomplishing the responsibilities set forth in this CJCSI. The Director, J-6, is responsible for:

(1) Serving as the GCCS Designated Approving Authority (GCCS DAA). The GCCS DAA's responsibilities are defined in Enclosure C.

(2) Appointing a GCCS Security Officer (GSO). The GSO's responsibilities are identified in Enclosure C.

c. The Director, DISA, provides the Joint Staff with all GCCS information systems support in accordance with guidance set forth in this CJCSI. The Director, DISA, is responsible for:

(1) Assisting the Joint Staff in implementing GCCS security policy.

(2) Ensuring proper GCCS certification is maintained.

(3) Providing day-to-day GCCS security operation support.

d. Chiefs of the Services, CINCs, Service components, and Directors of Defense agencies are responsible for:

(1) Appointing an official to serve as the GCCS DAA for the commander of Service, CINC, component or agency site. This official will be referred to as the GCCS Site DAA. GCCS site responsibilities are identified in Enclosure C.

(2) Ensuring that Site DAA's appoint Site GCCS Information System Security Officers (GCCS ISSOs) as described in Enclosure C.

(3) Ensuring that the Site DAA monitors operational objectives so that mission support with minimum response time does not conflict with the security objectives of maximum control and minimum risks.

7. Summary of Changes.

8. Effective Date.

Enclosure(s):

A--System Classification
B--Minimum Security Requirements
C--Responsibilities
D--Network Security
E--References
Glossary

DISTRIBUTION

(This page is used only when special distribution is necessary.)

Distribution A, B, C, and J plus the following:

	<u>Copies</u>
Secretary of State	2
Secretary of Defense	10
Director of Central Intelligence	20

LIST OF EFFECTIVE PAGES*

(This page is used only when instruction is 50 or more pages.)

The following is a list of effective pages for CJCSI 6731.01. Use this list to verify the currency and completeness of the document. An "O" indicates a page in the original document.

PAGE	CHANGE	PAGE	CHANGE
1 thru 4	O	H-1 thru H-20	O
i thru xi	O	I-1 thru I-64	O
A-1 thru A-2	O	J-1 thru J-36	O
A-A-1 thru A-A-4	O	K-1 thru K-8	O
A-B-1 thru A-B-8	O	L-1 thru L-4	O
A-B-A-1 thru A-B-A-2	O	M-1 thru M-2	O
B-1 thru B-32	O	M-A-1 thru M-A-2	O
C-1 thru C-20	O	M-B-1 thru M-B-2	O
D-1 thru D-8	O	N-1 thru N-6	O
E-1 thru E-8	O	O-1 thru O-2	O
F-1 thru F-4	O	GL-1 thru GL-4	O

(INTENTIONALLY BLANK)

(This page is used only when instruction is 50 or more pages.)

RECORD OF CHANGES

[illegible]

(INTENTIONALLY BLANK)

ENCLOSURE A

SYSTEM CLASSIFICATION

1. Mission Overview. The mission of the GCCS is to offer the warfighter—down to the joint task force (JTF) component commander, National Command Authorities, Joint Staff, Unified or Specified Commands, Services, and Defense agencies—a highly mobile, deployable, command and control system that offers a fused, real-time, true representation of the battlespace. It will be a comprehensive, global system to provide warfighters with a flexible and interoperable information system to support command and control requirements anytime and anywhere. The system will use the Defense Information System Network (DISN) for inter-site connectivity, and process up to SECRET information, TOP SECRET for GCCS(T), with functional users cleared for information at or above that level. The system must also work over tactical communications systems, which might not be physically connected to the larger network of GCCS sites, or must work during Power Projection Operations. To ensure effective command and control of military operations, the GCCS will be operated in command centers at the Pentagon, commander in chief, and JTF headquarters, and at the deployed Service component operations centers, as applicable. In successive releases, the GCCS will include additional capabilities that are interoperable and may require more extensive connectivity.

2. GCCS definition. Throughout this document, the term GCCS, refers to GCCS SECRET and GCCS(T) unless otherwise specified.

3. GCCS Classification. GCCS is classified as a SECRET US only level system functioning at a System High security mode of operation. GCCS(T) will be classified as a TOP SECRET US only level system functioning at a System High security mode of operation. GCCS(T) will contain all safeguards to ensure that TOP SECRET access is handled in accordance with DOD and NSA guidelines. Focal point is the only special category on GCCS. Specific procedures for use of focal point in GCCS is outlined within CJCSM 6731.01.

a. SECRET - the unauthorized disclosure of this information or material could reasonably be expected to cause serious damage to the national security.

b. TOP SECRET - the unauthorized disclosure of this information or material could reasonably be expected to cause exceptionally grave damage to the national security.

c. US only - access is restricted to personnel holding a final US SECRET clearances, interim or final US TOP SECRET for GCCS(T), and authorized

under the National Disclosure Policy and DOD 5230.11. Unless specifically annotated, the releasability of information residing on GCCS is governed by CJCSI 5714.01

d. System High security mode of operation is defined wherein all users having access to GCCS possess a final US SECRET security clearance or authorization as well as documented formal access approval, but not necessarily a need-to-know, for all data handled by GCCS. In the case of GCCS(T), all users having access must possess an interim or final US TOP SECRET security clearance or authorization as well as documented formal access approval, but not necessarily a need-to-know, for all data handled by GCCS(T). In operating at the System High security mode, GCCS and GCCS(T) must have a technical capability to control access to information based on a user's need to know.

4. Controlled Access Protection. GCCS operates at a C2 level of discretionary protection.

- a. System Access Control. Access to GCCS must be controlled, protected, and authorized only by a site designated office of primary responsibility.
- b. Accountability. Individual user accountability will be provided by GCCS, including authentication, unique identification, and auditing actions of the user.
- c. Assurance. GCCS will incorporate a capability to protect internal data and programs from unauthorized access or tampering.
- d. Documentation. GCCS will include a security features user's guide (SFUG) and a trusted facility manual (TFM) so that the security environment of GCCS can be appropriately established and maintained.
- e. Discretionary Access Control. Access to GCCS files must be controlled, protected, and authorized only by the owner of the files. The owner must verify the requester's need to know and clearance for the information.

ENCLOSURE B

GCCS MINIMUM SECURITY REQUIREMENTS

1. General Security Policy.

a. All GCCS information is classified SECRET, or TOP SECRET in the case of GCCS(T), (until determined otherwise) and will be protected in accordance with the provisions of DOD 5200.1-R. Safeguards will be applied to ensure that GCCS information and equipment is only accessed by authorized personnel, used only for its intended purpose, retains its content integrity, and is marked in accordance with DOD 5200.1-R.

b. Safeguarding of GCCS information and its resources (against sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse, or release to unauthorized persons) will be accomplished through the continuous employment of safeguards consisting of administrative, procedural, physical and/or environmental, personnel, communications security, emanations security, and computer security (i.e., hardware, firmware, and software), as required. The mix of safeguards selected will achieve the requisite level of security or protection.

c. The safeguards selected for GCCS will ensure that GCCS meets the minimum requirements as set forth in DODD 5200.28, Enclosure 3. These minimum requirements will be met through automated and manual means in a cost-effective and integrated manner. An analysis will be performed (e.g., using DODD 5200.28, Enclosure 4 or CJCSM 6731.01) to identify any additional requirements over and above the set of minimum requirements.

d. Computer security features of commercially produced products and Government developed or derived products will be evaluated (as requested) for designation as trusted computer products for inclusion on the NSA's Information Systems Security Products and Services Catalogue. Evaluated products will be designated as meeting security criteria maintained by the National Computer Security Center (NCSC) at NSA defined by the security division, class, and feature described in DOD 5200.28-STD or applicable documents for networks and databases. Products (operating systems, database management systems, network operating systems) used within GCCS shall to the maximum extent possible provide controlled access protection functionality (e.g., TCSEC class C2 controlled access protection functionality).

e. The interfacing and networking of GCCS with other Service and agency AISs are approved by the Joint Staff and controlled by the Service or agency. Site DAAs may authorize the networking of local LANs and AISs with GCCS at the appropriate classification level and subject to the restrictions of this security policy. Networks supporting GCCS(T) must not be connected to local LANs until approved NSA devices are available to support this multi-level security requirement and subsequent security policy is published by the Joint Staff. Such connections must be supported by an MOA executed by the site DAA and the connecting network/AIS DAA, or a memorandum of understanding (MOU) if the DAA is the same person. The Joint Staff must be notified of any MOAs/MOUs executed by the site and all MOAs/MOUs must be documented in the site accreditation. If the safeguards employed in the two systems differ significantly, the site may require reaccreditation.

f. All GCCS-related systems/program changes must be supported by DOD and GCCS security policies. Changes include, but are not limited to:

- (1) All applications/modifications.
- (2) All common operating environment (COE) modifications that impact GCCS.
- (3) All risks assumed by the sites in accrediting GCCS locally.

All changes to GCCS must be reviewed for type certification by DISA prior to implementation at sites. If recertification is required, then a type certification will be performed.

g. DISA is the system engineer and integrator for GCCS and is responsible for ensuring new releases, versions, segments, or patches comply with the trusted facility manual (TFM). This must include early and continuous involvement with the site users, GCCS ISSOs, data owners, and DAA(s) in defining and implementing security requirements of the AIS. There will be an evaluation plan for GCCS showing progress toward meeting full compliance with stated security requirements through the use of necessary computer security safeguards.

h. Mandatory statements of safeguard requirements will be included, as applicable, in the acquisition and procurement specifications for GCCS. The statements will be the result of a risk assessment, and will (to the extent possible) identify the functional security

requirement statements based upon the indicated level of trust required under DOD 5200.28-STD.

- i. The accreditation of GCCS will be a "type" accreditation from the Joint Staff supported by a certification plan, a risk analysis of GCCS in its operational environment, an evaluation of the security safeguards, and a certification report, all approved by the GCCS DAA. Each site will take the "type" accreditation and apply local requirements (i.e., configuration, environmental impacts, etc.) to complete a local accreditation for approval by the local site DAA. For the initial operation of GCCS, only the SECRET portion will be included in the accreditation. The TOP SECRET portion will be incorporated when functionality is delivered by developers, and evaluated for security safeguards.
- j. A program for conducting periodic reviews of the adequacy of the safeguards for the operational and accredited GCCS will be established. To the extent possible, reviews should include persons who are independent of the user organization and the GCCS operation or facility. At a minimum, this periodic review must be done at the 3-year accreditation point.
- k. Changes affecting the security of the GCCS type accreditation must be anticipated. Any changes to GCCS or associated environments that affect the accredited safeguards or result in changes to the prescribed security requirements will require DISA recertification and JS reaccreditation. Reaccreditation will take place before the revised system is declared operational.
- l. Procedures are established and documented by a configuration management plan to ensure that configuration management is performed in a specified manner and in accordance with the GCCS configuration management policy in CJCSI 6722.01. Configuration management ensures changes take place in an identifiable and controlled environment, and do not adversely affect any properties of the system. Configuration management provides assurance that additions, deletions, or changes made to the system do not compromise the trust of the originally evaluated system. CJCSI 6722.01 defines how applications, data, and equipment are approved for use by the Joint Staff, and how they are introduced into GCCS for use by the sites.
- m. A program for developing and testing contingency plans and recovery procedures will be established. The objective of contingency

planning is to provide reasonable continuity of GCCS support if events occur that prevent normal operations. The plans should be tested periodically under realistic operational conditions.

n. All GCCS users will possess a final US SECRET clearance, or in the case of GCCS(T) an interim or final US TOP SECRET clearance. GCCS will be operated in accordance with the National Disclosure Policy (NDP). Anyone requesting a waiver to the NDP must submit it to the Joint Staff, J3, for approval. J3 will forward it to the Joint Staff, J6V, for review and implementation. Contractor personnel must possess the appropriate clearance level as detailed in the CJCSM 6731.01. Data access is approved or granted by local functional managers and restricted to incidental access only. Contractors must be controlled and monitored through appropriate tasking from US Government employees, sufficient Government oversight as defined and provided by the site, and review of contractor deliverable products.

o. The site GCCS ISSO is responsible for ensuring that proper safeguards are in effect to restrict access to GCCS. The site GCCS ISSO, therefore, will be responsible for controlling all global access mechanisms to include such items as ROOT and world permissions.

p. Classification guidelines for the operation of GCCS will be included in CJCSM 6731.01.

q. Security incidents and violations will be reported in accordance with local security SOPs, and to DISA ASSIST and the Joint Staff, J6V.

2. GCCS Minimum Security Requirements. The following minimum requirements will be met through automated or manual means in a cost-effective manner and integrated fashion:

a. Accountability. There will be safeguards in place to ensure each person having access to GCCS will be held accountable for their actions. There will be an audit trail providing a documented history of GCCS use. The audit trail will contain sufficient detail to reconstruct events when determining if a compromise has taken place and if so, the severity and extent of the compromise. To fulfill this requirement, the manual and/or automated audit trail will document:

(1) The identity of each person and device having access to GCCS. Each authorized GCCS user and resource will have a unique system identity. Users will be required to identify and authenticate (e.g., passwords) themselves prior to accessing system resources.

Group accounts will be authorized by the local DAA. Group accounts will only be used for Joint Crisis Actions Teams (JCAT) and watch-team functions. Group accounts are not intended to replace individual user accounts and must provide individual accountability. Procedures for access to other sites are defined in CJCSM 6731.01.

(2) The time of access. Each individual user log on and log off will be audited.

(3) Specific User Activity (audit flags to be used as a minimum are specified in CJCSM 6731.01 and the TFM). These activities will be sufficient to ensure user actions are controlled and open to scrutiny. The audit events will include login/logout, selected administrative actions, or changes in security events, failed deletion events, and failed read/write as a minimum. Each site may include additional events as dictated by mission requirements.

(4) Activities that might modify, bypass, or negate safeguards controlled by the system.

(5) Audit records will be retained for a period of two (2) years or longer as directed by service or command requirements.

b. Access. There shall be in place an access control policy for each GCCS site. It shall include features and/or procedures to enforce the access control policy of the information within GCCS. The identity of each user requesting access to GCCS shall be positively established before authorizing access.

c. Security Training and Awareness. There will be in place a GCCS security education, training, and awareness program covering the security needs of all persons accessing GCCS servers and clients. The program shall ensure that persons responsible for GCCS and its information are aware of proper operational and security-related procedures and risks. Security awareness of GCCS should be incorporated into each site's annual security awareness program. The GCCS Concept of Operations (CONOPS) defines the single agency manager for training to support all sites.

d. Physical Controls. GCCS hardware, software, and documentation, and all its data shall be protected to prevent unauthorized (intentional or unintentional) disclosure, destruction, or modification (i.e., data integrity shall be maintained). The level of control and protection

shall be commensurate with the guidelines for SECRET information or in the case of GCCS(T), TOP SECRET information. This includes having personnel, physical, administrative, and configuration controls. Additionally, protection against denial of service of GCCS resources (e.g., hardware, software, firmware, and information) shall be consistent with the sensitivity of the information handled by the AIS.

- (1) DOD Executive Agents of GCCS software applications shall employ some means of physical controls within the respective developmental activity.
- (2) GCCS software, equipment and data, once installed, are classified at the Secret level, in the case of GCCS(T) at TOP SECRET, and both must be protected in accordance with the requirements set forth in DOD 5200.1-R.
- (3) All GCCS equipment shall be implemented in a secure room as outlined in Appendix G of DOD 5200.1-R. This includes permanently constructed walls and ceilings that are attached with mesh or 18-gauge expanded steel screen. Doors shall be substantially constructed of wood or metal. Hinge pins of out swing doors shall be peened, braised, or spot welded to prevent removal. Doors shall be equipped with a built-in GSA-approved combination lock meeting federal specification FF-L-2740. Windows which are less than 18 feet above the ground measured from the bottom of the window, or are easily accessible by means of objects directly beneath the window shall be constructed from or covered with materials which will provide protection from forced entry. The protection provided to the windows need be no stronger than the strength of the contiguous walls. Due to the critical nature of servers within GCCS, strongly recommend that all servers be inaccessible except through controlled means. Examples are: locked in a secure closet in a secure room; locked in a cable/telephone closet in a secure room; or, in a locked cabinet in a secure room. The importance of restricting physical access to any GCCS server cannot be overemphasized.
- (4) For protection of TOP SECRET information in a secure room, an intrusion detection system (IDS) must be installed in accordance with Appendix G, DOD 5200.1-R. This will be required for all workstations accessing the TOP SECRET portion of GCCS.
- (5) For protection of SECRET information in a secure room, an

IDS is not required per DOD 5200.1-R. All GCCS equipment that does not handle or access TOP SECRET information does not require installation at the same level as for TOP SECRET as described above.

(6) Entrance to secure rooms or rooms controlled by IDS should be visible at all times or equipped with electric, mechanical, or electromechanical access control devices to limit access during duty hours. Electrically actuated locks (e.g., cipher and magnetic strip card locks) do not afford, by themselves, the required degree of protection for classified information. DOD 5200.1-R Appendix G further defines standards for access control devices.

(7) In field and combat operations, the provisions of this policy pertaining to accountability, dissemination, transmission, and storage of classified information and material may be modified by military commanders who are responsible for ensuring adequate security is maintained for GCCS.

e. Marking. GCCS output shall be marked to accurately reflect the sensitivity of the information. Requirements for security classification and applicable markings for classified information are set forth in DOD 5200.1-R. The markings may be automated or may be done manually. Automated marking on output must not be relied on to be accurate, unless the security features and assurances of the AIS meet the minimum requirements for a security class of B1 as specified in DOD 5200.28-STD. If B1 is not met, but automated controls are used, all output shall be protected at the SECRET, or in the case of GCCS(T) at the TOP SECRET, system high level until manually reviewed by an authorized person to ensure that the output was marked with the proper classification and caveats. All media (and containers) shall be marked and protected at the SECRET, or TOP SECRET for GCCS(T), system high level until the media are declassified (e.g., degaussed or overwritten) using a DOD-approved methodology or in accordance with NCSC-TG-025, A Guide to Understanding Data Remanence in Automated Information Systems, or unless the information is declassified or downgraded in accordance with DOD 5200.1-R.

f. Least Privilege. GCCS shall function so that each user has access to all of the information to which the user is entitled (by virtue of clearance, formal access approval), but to no more. In the case of "need-to-know" for GCCS information, access must be essential for accomplishment of lawful and authorized Government purposes.

- g. Data Continuity. Each file or data collection in GCCS shall have an identifiable source throughout its life cycle. Its accessibility, maintenance, movement, and disposition shall be governed by security clearance, formal access approval, and need-to-know.
- h. Data Integrity. There shall be safeguards in place to detect and prevent inadvertent modification or destruction of data, and detect and prevent malicious destruction or modification of data.
- i. Contingency Planning. Contingency plans shall be developed and tested in accordance with OMB Circular No. A-130 to ensure that GCCS security controls function reliably and, if not, that adequate backup functions are in place to ensure that security functions are maintained continuously during interrupted service. If data is modified or destroyed, procedures must be in place to recover.
- j. Accreditation. GCCS shall be accredited to operate in accordance with a DAA-approved set of security safeguards. Each GCCS site will be accredited for local operations by the site DAA.
- k. Risk Management. A risk management program will be implemented to determine how much protection is required, how much exists, and the most economical way of providing the needed protection.
- l. GCCS does not require TEMPEST configurations. However, if the CJTF or CINC determines TEMPEST is required to accomplish their mission, the Vice J6, Joint Staff, must be notified. Procedures for implementing TEMPEST configurations are found in CJCSM 6731.01.
- m. Scheduled shutdown and restart during a processing period will follow procedures described in the CJCSM 6731.01.
- n. Clients (workstations) will be operated, at a minimum, with the functionality of a TCSEC class of C2. If a site cannot achieve a C2 status, a JS waiver must be requested, and as a minimum, need to know separation of data will be maintained.
- o. Waiver authority can be found in Appendix F, Security Policy Waiver Authority. Waivers for any aspects of this security policy will be forwarded to the Joint Staff, J6V, either for approval or notification. Sufficient documentation must accompany all waiver requests and be included in the site's certification and accreditation documentation.

p. Increased security for PCs and other workstations will be improved in each future version of GCCS. Details on the specifics of increased security for workstations in each GCCS release will be updated and incorporated into CJCSM 6731.01 immediately following each GCCS version change or update. Examples may include screen lockout, stricter system access through WS and other lockout capabilities.

(INTENTIONALLY BLANK)

ENCLOSURE C
RESPONSIBILITIES

1. Director J-6, Joint Staff.

a. GCCS Designated Approving Authority. The GCCS DAA responsibilities include:

- (1) Reviewing and approving security safeguards for the GCCS.
- (2) Issuing type accreditation statements based on the acceptability of the GCCS security safeguards.
- (3) Approving GCCS site connections to non-GCCS systems.
- (4) Ensuring that all safeguards required, as stated in the GCCS type accreditation documentation, are implemented and maintained.
- (5) Identifying security deficiencies and, where the deficiencies are serious enough to preclude type accreditation, taking action to achieve an acceptable security posture.
- (6) Ensuring that a GSO is named for the GCCS, and that the GSO receives the necessary training to carry out the duties of this function.
- (7) Requiring that a GCCS security education, training and awareness program must be in place.
- (8) Ensuring that information ownership is established for the GCCS, to include accountability, access rights, and special handling requirements.
- (9) Establishing MOAs with Site GCCS DAAs of external non-system wide AISs connected to GCCS.
- (10) Approving the Security Policy for GCCS.

b. GCCS Security Officer. The GSO is the primary staff officer reporting to the GCCS DAA. The GSO manages the GCCS security program. GSO responsibilities include:

- (1) Implementing and managing the GCCS information systems security program.
- (2) Developing and maintaining the GCCS security policy and procedures.
- (3) Implementing and managing the GCCS DAA-approved security policy and procedures.

- (4) Acting as the GCCS DAA and GCCS ISSO information systems security advisor.
- (5) Reviewing all GCCS type accreditation submissions and preparing accreditation recommendations for the GCCS DAA.
- (6) Serving as a voting member of the GCCS Configuration Control Board (CCB) as defined in CJCSI 6722.01, GCCS Configuration Management Policy. The GSO will have the primary responsibility for providing information to the CCB Director on the expected security impact of all proposed system changes to be made to the CCB.
- (7) Maintain this Instruction and publish amendments and changes as approved by the Joint Staff.
- (8) Investigate and resolve security related issues and incidents involving GCCS.

2. Site-Based Responsibilities.

a. Site GCCS Designated Approving Authority. The Site GCCS DAA responsibilities include:

- (1) Reviewing and approving security safeguards for the site GCCS components.
- (2) Issuing site accreditation statements based on the acceptability of the GCCS security safeguards.
- (3) Ensuring that all safeguards required, as stated in the GCCS site accreditation documentation, are implemented and maintained.
- (4) Identifying security deficiencies and, where the deficiencies are serious enough to preclude site accreditation, taking action to achieve an acceptable security posture.
- (5) Ensuring that a GCCS ISSO is named for the site GCCS and that the GCCS ISSO receives applicable training to carry out the duties of this function.
- (6) Requiring that a site GCCS security education, training, and awareness program must be in place.
- (7) Ensuring that information ownership is established for the site GCCS components, to include accountability, access rights, and special handling requirements.
- (8) Establishing MOAs or MOUs, if the DAA is the same for both

components, with DAAs of external information systems and/or networks remotely connected to the site GCCS to ensure the continued security of sensitive information.

(9) Establishing MOAs with the GCCS DAA when the site GCCS components are connected to non-GCCS site systems.

(10) Approving GCCS site connections to non-GCCS SECRET systems, or TOP SECRET systems in the case of GCCS(T), in coordination with the GCCS DAA.

(11) Approving the GCCS Site Security Policy.

(12) Ensuring that all information system security incidents or violations are investigated and that appropriate corrective action is taken.

(13) Ensuring that the site GCCS components are accredited for operational use.

(14) Ensuring the development and testing of site contingency plans.

(15) Reporting to J6V, any site security anomalies that may adversely affect the GCCS network or servers.

(16) Creating proper organizational placement for the site GCCS ISSO. The site GCCS ISSO will ensure maximum security objectives are attained with minimum impact to mission requirements and operational performance. For example, assigning the site GCCS ISSO to internal subordinate organizations hampers adequate security accomplishment and is therefore considered a security risk.

b. Site GCCS Information System Security Officer (GCCS ISSO). Reporting to the GCCS Site DAA, the GCCS ISSO is the site's senior information security official in the absence of a site GCCS Information System Security Manager (ISSM). The GCCS ISSO manages the site's GCCS security program. The GCCS ISSO responsibilities include:

(1) Developing, implementing, and managing of the site's GCCS information systems security program, to include security education, training, and awareness.

(2) Developing and maintaining the site's GCCS Site Security Policy and procedures.

(3) Performing site certifications for GCCS.

(4) Functioning as the operational arm of the Site DAA in implementing and managing the GCCS Site approved Security Policy and Procedures.

- (5) Is the GCCS Site DAA information systems security adviser in the absence of an ISSM.
- (6) Developing all GCCS site accreditation submissions and preparing accreditation recommendations for the GCCS Site DAA.
- (7) Monitoring the site GCCS equipment usage for unauthorized or improper activity (e.g., audit review and intrusion detection).
- (8) Supervising and testing all site GCCS equipment and software changes.
- (9) Investigating and reporting all GCCS site security violations to the GCCS Site DAA, or J-6V if outside the site's environment.
- (10) Ensuring that personnel, who use the GCCS, hold proper clearances and access authorizations that are current and valid.
- (11) Performing periodic security audits of the GCCS.
- (12) Performing password management.
- (13) Qualification. A U.S. Government employee capable of ensuring GCCS security policy and guidance in this publication and other directives have been properly implemented. This position will not be filled by contractor personnel.

3. Additional Security Support. In addition to the roles identified above, the GCCS Site DAA and the GCCS ISSO may designate subordinate roles and responsibilities as necessary to implement an information system security program at their site. These may include but are not limited to GCCS ISSMs, Assistant GCCS ISSOs, Site GCCS Coordinators, and Site GCCS Data Base Managers.

4. GCCS ISSM. The GCCS ISSM is assigned at the discretion of the local DAA for overall security management of a single site or multiple sites.

Responsibilities include:

- a. Security policy implementation and security oversight responsibilities at single or multiple sites.
- b. Coordination of GCCS security measures including analysis, testing, evaluation, verification, accreditation, and review of GCCS installation at the appropriate classification level within the site's network structure.
- c. Ensuring security instructions, guidance, and standard operating procedures are prepared and maintained at each site.

d. Monitor implementation of security guidance and direct action appropriate to remedy security deficiencies.

e. Qualification. A U.S. Government employee capable of ensuring GCCS security policy is implemented and enforced. Experience in the application and enforcement of information and ADP security measures, threats, and vulnerabilities. This position will not be filled by contractor personnel.

5. Defense Information Systems Agency (DISA). DISA is the primary integration agent for GCCS. DISA responsibilities include:

a. Providing centralized security technical support for the development, maintenance, test, evaluation, and use of all components of GCCS.

b. Reviewing specifications for software and hardware security features.

c. Performing security evaluations for all software patches implemented between software releases.

d. Performing security test and evaluations (ST&Es) for standard software releases.

e. Evaluating problem reports/change requests for security and provide results to the J-6, Joint Staff.

f. Evaluating GCCS security incident reports that deal with technical and system software issues and provide recommendations to the GSO.

g. Perform security tests on standard GCCS hardware and software as required by J-6, Joint Staff, as defined in the DISA Type Certification.

h. Developing, installing, analyzing, testing, and evaluating prototype AIS security protection systems for GCCS in conjunction with the appropriate Services, unified and specified commands, and Defense agencies.

i. Providing software capable of declassifying and regrading standard GCCS hardware and removable media. Certifies to the J-6, Joint Staff, that this software performs as specified before field use and serves as its configuration manager. Provides a list of this software to all GCCS ISSOs.

j. Supporting the GSO by maintaining technical cognizance of all aspects of computer network security, including hardware, software, COMSEC, and EMSEC.

k. Evaluating specialized ST&E tools for use with GCCS.

l. Providing written technical AIS security evaluations of GCCS certification documents to the GSO.

- m. Evaluating and distributing standard automated software security tools to GCCS sites to support the GCCS ISSO's implementation of this instruction as identified in CJCSM 6731.01, Security Procedure Manual
- n. Reviewing and providing technical support for procedures and security measures for the GCCS security Procedures Manual, CJCSM 6731.01.
- o. Evaluating site-submitted software patches for operational effectiveness, security impact, etc.
- p. Providing a technical analysis of security bulletins such as ASSIST, CERT, FIRST, and SUN, etc. that impact GCCS software.
- q. Providing recommended modifications to GCCS software in accordance with applicable security bulletins such as ASSIST, CERT, FIRST, and SUN, etc.
- r. Ensure the type certification supports sufficient C2 compliant testing for all hardware, software (operating systems and applications) and firmware in GCCS.

6. GCCS User Security Responsibilities. Each GCCS user has security responsibilities. They include (but are not limited to):

- a. Using the system only for authorized, official purposes.
- b. Maintaining individual accountability. Ensuring all operations are under assigned user account. Making no attempt to change or mask assigned user identity. Being responsible for all activity that occurs under the assigned user account.
- c. Changing access passwords as directed, minimum every 90 days, in accordance with local security Standard Operating Procedures (SOP) provided by the site GCCS ISSO. Protecting the SECRET password which authenticates the user by:
 - (1) Changing the account password immediately after the first log in.
 - (2) Not permitting anyone else to use the assigned user account.
 - (3) Not revealing individual passwords to anyone else at any time.
 - (4) Storing passwords only in authorized locations, classified as SECRET.
- d. Ensuring that output products are marked or downgraded in accordance with the GCCS security policy. Safeguarding classified and sensitive unclassified input/output data. Safeguarding, reporting, and returning

- unexpected or unrecognizable output according to local security SOP.
- e. Not entering data into the system if the data is of a higher classification level than the system (SECRET and TOP SECRET for GCCS(T)).
 - f. Protecting classified and other sensitive material. Protecting all system output at the system-high level (SECRET or TOP SECRET for GCCS(T)) until reviewed as to actual classification (based on content), and appropriately downgraded by an approved process. Marking (label) all hardware and output with labels unless properly downgraded. Safeguarding terminals and workstations located in their respective areas.
 - g. Using only secure (US SECRET and US TOP SECRET for GCCS(T)) communications links.
 - h. Not leaving GCCS terminals unattended and signed on.
 - i. Not moving hardware, or altering communication connections without prior approval from appropriate local network configuration personnel. Maintaining minimum physical separation of system components in accordance with service red/black (TEMPEST) standards.
 - j. Checking all diskettes for viruses before loading on GCCS.
 - k. Complying with all security guidance in this policy and in local security SOP.
 - l. Promptly reporting any system security abuses, abnormalities, discrepancies, incidents, vulnerabilities, or any other situation which indicates inadequate security to the area security officer and the site GCCS ISSO.
 - m. Operating the system reliably. Using the system only as configured by the System Administrator.
 - n. Not attempting to access files or data, or use operating systems programs, except as specifically designed or authorized.
 - o. Not installing any hardware or software (including importing or exporting of software). (Only System Administrators, in conjunction with the GCCS ISSO, can authorize and coordinate installation of additional software or hardware.)

(INTENTIONALLY BLANK)

ENCLOSURE D

NETWORK SECURITY

1. System Identification, Need, and Mission Overview.

a. The Defense Information Systems Agency (DISA) is leading the DOD effort to provide a modern, survivable, and secure DOD-wide, network of computers, communications, and data applications, that can evolve to meet changing user information requirements. This network initiative is driven by the DOD need for local and worldwide system interconnectivity, integration, and interoperability and encompasses the various systems that support DOD missions and functions. Collectively these systems are known as the Defense Information Infrastructure (DII). One subset of the DII is the Secret INTERNET Protocol Router Network (SIPRNET). The SIPRNET provides end-to-end information transfer and value added services, for the transport of data up to the secret level. This policy does not replace any security policy already in place. SIPRNET security requirements also apply to any service unique networks or subnetworks used to transmit GCCS data. Detailed information for SIPRNET configuration, control, management, etc., can be found in the system and network management CONOPS, DISN CONOPS, and SIPRNET operations guide.

b. The SIPRNET architecture supports National Defense Command, Control, Communications, Computers, and Intelligence (C4I) worldwide information transfer requirements. The SIPRNET is the secret level router-based Wide Area Network (WAN) of the Defense Information System Network (DISN). Before creation of the SIPRNET, DOD maintained the DDN for DOD users worldwide. The DDN consisted of four packet-switched networks that were physically separated and identified according to the classification level of the data transported. The Secret system high network portion of DDN was called Defense Systems Network 1 (DSNET1). In response to technological changes and a changing subscriber base, the DISN concept was established. The DISN's goal is to evolve into a worldwide information transfer infrastructure supporting long haul requirements. SIPRNET was the first of the three DISN router layers to become operational under common management by DISA. The SIPRNET supports those subscribers who were on the old style X.25 packet switching technology of the DDN DSNET1. SIPRNET will build on the following DISN initiatives for users of end systems:

- (1) High speed packet switching using INTERNET Protocol (IP) routers and asynchronous switching using Asynchronous Transfer Mode (ATM) switches.
- (2) Circuit multiplexing using remotely managed smart multiplexers.
- (3) Bundling access, trunk, and individual circuits for economies of

scale.

(4) Integration and consolidation of network management and customer support.

c. The SIPRNET consists of routers, switches, hubs, communications servers, multiplexers, encryption devices, three Regional Control Centers (RCC), one Global Control Center (GCC), one SIPRNET Support Center (SSC), a baseline of host connections, and Integrated Tactical Strategic Demonstration Network (ITSDN). The ITSDN was created to support a DOD requirement, to be able to conduct two contingency operations in different parts of the world simultaneously. The ITSDN Quick Fix Program installed gateway routers to support deployed Joint Task Force (JTF) contingencies, exercises, and training missions with requirements to interface with the DISN INTERNET Protocol Routers (IPR). Deployed GCCS forces may rely on the ITSDN capabilities to reach the SIPRNET WAN. SIPRNET will provide high speed Software applications through the use of INTERNET Protocol (IP) routers. This high speed datagram service is primarily intended to satisfy a large number of aggregated subscriber requirements coming from a multitude of local area and wide area networks, or subscriber premise routers. Subscriber connection requirements vary from those needing a sophisticated level of INTERNET routing support (such as complex subscriber domains with multiple routers, networks, and connections) to those needing a very simple routing interface (such as a host). SIPRNET subscribers can be divided into four basic groups:

(1) Dedicated subscribers, users on computers (mainframe hosts, PCs, terminals) that are directly connected to the SIPRNET backbone routers via serial, Ethernet, and Fiber Distributed Data Interface (FDDI) lines, and Synchronous Optical Network (SONET) lines.

(2) Dial up subscribers, users who do not have the need for dedicated connections, as well as travelers on TDY. These users can access SIPRNET via approved STU III's, as discussed in section 6.0, "Reports of Evaluated Products."

(3) Tactical subscribers, users that gain access to the SIPRNET via the ITSDN. Tactical forces are allowed access to the SIPRNET, as well as other tactical networks via the Defense Satellite Communications System (DSCS), Global Broadcast Service (GBS), and MILSTAR through a Standard Tactical Entry Point (STEP).

(4) External Network Subscribers, users on networks such as AFNET and NIPRNET who require access to the SIPRNET. Connections between Unclassified and Secret users are approved for unclassified e-mail only. A Secure Network Server (SNS) that incorporates a Standard Mail Guard (SMG) application is available for procurement by users to facilitate the

unclassified e-mail requirement.

d. GCCS local networks consist of routers, switches, hubs, communications servers, multiplexers, and encryption devices. This network of LANs and WANs connect GCCS users and non-GCCS users to the GCCS servers and/or the SIPRNET. It is the responsibility of the site DAA and site GCCS ISSO to ensure the security of the GCCS local networks and to forward their accreditation to the GSO for approval. For those sites from which GCCS has been incorporated into the local backbone LAN structure, additional security enforcement must be provided to ensure GCCS does not experience a denial of service. Integrating GCCS into the local LAN structure increases the security management and implementation controls at the site that would not normally be required of the site to provide if GCCS had been implemented as a separate network structure. GCCS(T) LAN structures will not be connected to any lower classified network until an NSA approved multi-level security device is available and the amended security policy published by the Joint Staff.

2. Network Security Policy.

a. The GCCS SIPRNET and GCCS local network security policy is based upon DODD 5200.28, which is the primary document governing security policy for all DOD automated information systems (AIS), including communication systems and computer network systems of all sizes. DODD 5200.28 establishes responsibilities for implementing AIS security programs for all long-haul DOD networks and defines requirements for protection of SECRET information. Director, DISA, is responsible for accrediting networks that handle all general service (GENSER) data. Since SIPRNET is a subnet of the DISN, the Designated Approving Authority (DAA) responsibilities are shared by four DOD organizations. They are the Directors of DISA, National Security Agency (NSA), Defense Intelligence Agency (DIA), and Joint Staff (JS).

b. GCCS Network Security Concept of Operations

(1) SIPRNET and GCCS local network users must comply with the DISN security policy and applicable National, DOD, service, and agency security policies. In general, SIPRNET and the GCCS local network will process and protect all classified and/or sensitive information from unauthorized disclosure, modification and destruction. DISA's responsibility ends at the encryption device and access circuit connecting the subscriber's host, LAN or premise Router to the SIPRNET. SIPRNET users will be accredited to operate at the security level of the corresponding network, however, they must take care to never compromise SIPRNET security or integrity. GCCS user information falls within the category covered by DODD C-5200.5, Communications Security, dated 21 April 1990. As such, only NSA endorsed products,

techniques, and protected services shall be used to protect SIPRNET access lines.

(2) A GCCS LAN is described as a network which contains a GCCS management server, and includes any connection to a network that contains a GCCS management server. It also includes workstations that are connected to another network which contains a GCCS management server except when those connections are controlled by a STU III secure device or a communications server requiring full identification and authentication access.

(3) Confidentiality. DISA is responsible for ensuring the SIPRNET protects information/data in transit up to the SECRET level. In the case of GCCS(T), encryption devices will be used to prepare data for transit at the SECRET level over SIPRNET. SIPRNET and the GCCS local network will effect means necessary to prevent unauthorized information disclosure/dissemination.

(4) System Integrity. DISA will ensure that controls are in place to prevent unauthorized SIPRNET and the GCCS local network configuration modification.

(5) Data Integrity. Encryption provides the checksum used to ensure data integrity. SIPRNET, the GCCS local network, and the end system share responsibility for user data integrity. It is generally recognized that the end-user system is responsible for detecting and recovering information that may have been damaged or altered by the communication process through the transport service. However, SIPRNET bears total responsibility for network control data.

(6) Identification, Authentication and Access Control. The SIPRNET does not have the capability to authenticate or control access for users of attached end systems. It will be the end user's responsibility for Identification and Authentication (I&A). SIPRNET and the GCCS local network will protect against external accesses to the information or system by encryption.

(7) Non-repudiation. SIPRNET and the GCCS local network do not protect against a sender's attempt to falsify information origination (i.e., proof of origin).

(8) Availability. SIPRNET and the GCCS local network will ensure uninterrupted user access to authorized functions and information.

(9) Network Security. Classified or sensitive information in clear text is not allowed to pass through the multiplexer layer or over individual circuits. All IP routers, X.25 packet switches, X.500 asynchronous switches, multiplexers and related components shall be protected at the

SECRET level. SIPRNET and GCCS local network users must protect all exposed trunks between IP routers and X.25 packet switches, and exposed subscriber access links to routers or switches with KG-type devices. The term exposed is defined as "exiting base, post, camp, or station boundaries."

(10) WEB Server Requirements. Management of WEB servers will be strictly controlled at all sites. Password management, information content, gateway interfaces, and permission sets will be controlled to support maximum utility of the WEB server while also ensuring adequate security controls in place. Each site should appoint an administrator to oversee WEB server functions, these functions may or may not be performed by the GCCS ISSO. Additional specific guidance is provided in CJCSM 6731.01.

3. Statements of Existing Accreditation and Waivers. DODD 5200.28 requires that all DOD AISs be accredited. All SIPRNET users are required to have an accreditation document as a condition for granting SIPRNET access.

4. Contingency Planning Requirements. In accordance with DODD 5200.28, all SIPRNET and GCCS local network users are required to develop a contingency plan, which will allow their AIS mission to continue in the event of abnormal operating conditions. Contingency plans must be tested to ensure that AIS security controls are effective, and function reliably during service interruptions. DISA is responsible for all contingency planning for SIPRNET. The contingency plan must include recovery procedures for modified or destroyed data. The contingency plan must address the following areas as a minimum:

- a. Actions required if the normal AIS environment is impaired or disrupted.
- b. Actions required if the functional application is denied information or service (Ex., application cannot access needed information files or is denied service).
- c. Users are denied information or service (Ex., user is denied application access).
- d. Actions required for an emergency or expanded operations.

5. Configuration Management Requirements. DISA is responsible for overall SIPRNET configuration management. SIPRNET users shall establish configuration management procedures to ensure that changes made to their system's hardware, software, firmware, documentation, tests, test fixtures, and/or test documentation occur in an identifiable and controlled environment. System changes must never adversely affect SIPRNET properties or DISN security policy implementation.

6. Reports of Evaluated Products. Per DODD C-5200.5, Communications Security, dated 21 April 1990, only NSA endorsed COMSEC products and services shall be used to secure classified telecommunications of DOD components and their contractors. Therefore only encryption devices listed in the "Endorsed Cryptographic Products List" of the "NSA Information Systems Security Products and Service Catalogue" are authorized for use. These products have been endorsed for use in securing SECRET US Government or Government derived information during its transmission. The DISN Program Management Office (PMO) provides all KG encryption technology as part of their service to the customer. SIPRNET users must provide their own encryption devices (e.g., STU III's) for use within their network.

7. Organization and Resources. The Director, Joint Staff J6, through the DISN Security Accreditation Working Group (DSAWG) will validate unified and specified command, Service, or Defense agency subnetworks for users requesting SIPRNET connectivity. Connectivity will normally be approved if residual risks, not covered by SIPRNET mechanisms and procedures, are sufficiently small to be outweighed by the operational benefits of network use.

ENCLOSURE E

REFERENCES

The following documents are either included in this document or are essential to the duties of AIS security officers. These documents include executive orders; DOD Directives, Instructions, and Standards; and Joint Staff Instructions and Manuals.

1. Executive Documents.

- a. Executive Order 12958, "Classified National Security Information"
- b. Executive Order 12333, "United States Intelligence Activities"
- c. Public Law 100-235, "The Computer Security Act of 1987"
- d. OMB Circular No. A-130, "Management of Federal Information Resources"
- e. OMB Circular No. A-123, "Internal Control System"
- f. Title 18, United States Code 1905, "Espionage Act," Section 793, "Gathering, Transmitting, or Losing Defense Information" and Section 794, "Gathering or Delivering Defense Information to Aid Foreign Government"
- g. Information Security Oversight Office (ISOO) Directive No.1, "National Security Information"
- h. ISSO, "Information System Security Organization Strategic Plan"
- i. Federal Register 32 CFR Part 2003, "National Security Information; Standard Forms; Final Rule" Part II ISOO

2. DOD Documents (NSA, DIA, DNA, DLA, DISA).

a. Information Security.

- (1) DOD Directive 5200.1, "DOD Information Security Program"
- (2) DOD Regulation 5200.1-R, "Information Security Program"
- (3) DOD Directive 5200.12, "Conduct of Classified Meetings"
- (4) DOD Directive 5200.21, "Dissemination of DOD Technical Information"
- (5) DOD Directive 5230.9, "Clearance of DOD Information for Public Release"

- (6) DOD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations"
- (7) DOD Directive C-5230.23, "Intelligence Disclosure Policy"
- (8) A DOD/ADUSD Memo, "Interpretation of the Two-Person Integrity Requirement of Paragraph 7-100b, DOD 5200.1-R, 'Information Security Program Regulation'"
- (9) DOD Instruction 7930.2, "ADP Software Exchange and Release"
- (10) DOD Directive 5400.7, "DOD Freedom of Information Act Program"
- (11) DOD Directive 5400.11, "Department of Defense Privacy Program"
- (12) DOD Directive 7920.1, "Life-Cycle Management of Automated Information Systems (AISs)"
- (13) NSA, "Information Systems Security Products and Services Catalogue," published quarterly.

b. Computer Security.

- (1) DOD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)"
- (2) DOD Manual 5200.28-M, "Automated Information System (AIS) Security Manual" (under revision).
- (3) DOD Standard 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria"

c. Operational Security.

- (1) DOD Directive 5205.2, "DOD Operations Security Program"
- (2) DOD Directive O-5205.7, "Special Access Program"
- (3) DOD Directive 5205.8, "Access to Classified Cryptographic Information"
- (4) DOD Directive 5210.2, "Access to and Dissemination of Restricted Data"
- (5) DOD Directive 5210.50, "Unauthorized Disclosure of Classified Information to the Public"
- (6) DOD Directive 5215.1, "Computer Security Evaluation Center"
- (7) DOD Directive 5215.2, "Computer Security Technical Vulnerability

Reporting Program (CSTVRP)"

(8) DOD Directive 3020.26, "Continuity of Operations Policies and Plans"

d. Communications Security and Emissions.

(1) DOD Directive C-5200.5, "Communications Security (COMSEC) (U)"

(2) DOD Directive S-5200.17, "The Security, Use and Dissemination of Communications Intelligence (COMINT) (U)"

(3) DOD Directive S-5200.19, "Control of Compromising Emanations (U)"

(4) DOD Directive 5210.74, "Security of Defense Contractor Telecommunications"

(5) DOD Directive 5240.5, "DOD Technical Surveillance Countermeasures (TSCM) Survey Program"

(6) DOD C-5030.58-M, "Defense Special Security Communications System: Security Criteria and Telecommunications Guidance"

e. Personnel Security.

(1) DOD Directive 5200.2, "DOD Personnel Security Program"

(2) DOD Regulation 5200.2-R, "DOD Personnel Security Program Regulation"

(3) DOD Directive 5220.6, "Defense Industrial Personnel Security Clearance Review Program"

f. Physical Security.

(1) DOD Directive 5200.8, "Security of Military Installations and Resources"

(2) DOD Directive 5220.22, "Industrial Security Program"

(3) DOD Regulation 5220.22-R, "Industrial Security Regulation"

(4) DOD Manual 5220.22-M, "Industrial Security Manual for Safeguarding Classified Information"

3. CJCS Instructions and Manuals

- a. CJCSI 3137.01, "The Joint Warfighting Capabilities Assessment Process"
- b. CJCSI 3213.01, "Joint Operations Security" (supersedes CJCS MOP 29)
- c. CJCSM 3213.02, "JCS Focal Point Communications System Procedures Manual" (supersedes SM-769-89)
- d. CJCSI 5714.01, "Release Procedures for Joint Staff and Joint Papers and Information" (supersedes CJCS MOP 60)
- e. CJCSI 6111.01, "Command, Control, Communications, and Computer Systems Master Plans, Assessments, and Evaluation" (supersedes CJCS MOP 50)
- f. CJCSI 6115.01, "Reduction, Realignment, and Contracting of Command, Control, communications, and Computer Facilities" (supersedes CJCS MOP 79)
- g. CJCSI 6210.01, "Command Center Systems Architecture and IPS Guidance" (under development)
- h. CJCSI 6211.01, "Defense Data Network and Connected Systems" (supersedes CJCS MOP 38) (under development)
- i. CJCSI 6211.02, "Defense Information System Network and Connected Systems" (supersedes CJCS MOPs 38 and 70)
- j. CJCSI 6212.01A, "Compatibility, Interoperability, and Integration of Command, Control, Communications, Computers, and Intelligence Systems"
- k. CJCSI 6215.01, "Policy for Defense Switched Network Service" (supersedes CJCS MOP 8)
- l. CJCSI 6510.01, "Joint and Combined Communications Security" (supersedes CJCS MOP 54)
- m. CJCSI 6620.01, "Policy and Procedures for the Management of Information Technology Standards used in Combined Operations" (under development)
- n. CJCSI 6721.01, "Global Command and Control Management Structure"
- o. CJCSM 6721.01, "Best of Breed Process for Global Command and Control Systems (GCCS) (under development)
- p. CJCSM 6721.02, "Global Command and Control System Technical Requirements Evaluation Procedures" (under development)

q. CJCSI 6722.01, "GCCS Configuration Management Policy"

r. CJCSM 6731.01, "Global Command and Control System (GCCS) Security Procedures Manual" (under development)

(INTENTIONALLY BLANK)

APPENDIX F

GCCS SECURITY POLICY WAIVER AUTHORITY

Waiver Authority

1. General Security Policy. The following requirements are waivable as indicated:

a. Computer security features of commercially produced products and Government developed or derived products will be evaluated (as requested) for designation as trusted computer products for inclusion on the NSA's Information Systems Security Products and Services Catalogue. Evaluated products will be designated as meeting security criteria maintained by the National Computer Security Center (NCSC) at NSA defined by the security division, class, and feature described in DOD 5200.28-STD or applicable documents for networks and databases. Products (operating systems, database management systems, network operating systems) used within GCCS will to the maximum extent possible provide controlled access protection functionality (e.g., TCSEC class C2 controlled access protection functionality).

b. All GCCS related systems/program changes must be supported by DOD and GCCS security policies. Changes include, but are not limited to:

(1) All applications/modifications.

Joint Staff

(2) All Common Operating Environment (COE) modifications that impact GCCS.

Joint Staff

c. All GCCS users will possess a final US SECRET clearance, or in the case of GCCS(T) an interim or final US TOP SECRET clearance. GCCS will be operated in accordance with the National Disclosure Policy (NDP). Anyone requesting a waiver to the NDP must submit a request to the Joint Staff, J3, for approval. J3 will forward the request to the Joint Staff, J6V, for review and implementation. Contractor personnel must possess the appropriate clearance level as detailed in the CJCSM 6731.01. Data access is approved or granted by local functional managers and restricted to incidental access only. Contractors must be controlled and monitored by US government employees.

Joint Staff

2. GCCS Minimum Security Requirements. The following minimum requirements will be met through automated or manual means in a cost-effective manner and integrated fashion:

a. Specific User Activity (audit flags to be used as a minimum are specified in CJCSM 6731.01 and the TFM). These activities will be sufficient to ensure user actions are controlled and open to scrutiny. The audit events will include login/logout, selected administrative actions, or changes in security events, failed deletion events, and failed read/write as a minimum.

b. Access. There will be in place an access control policy for each GCCS site. It shall include features and/or procedures to enforce the access control policy of the information within GCCS. The identity of each user requesting access to GCCS will be positively established before authorizing access.

GLOSSARY

Part I - Abbreviations and Acronyms

AIS	Automated Information System
ATM	Asynchronous Transfer Mode
B1 level)	Labeled Security Protection (TCSEC criteria
C2 level)	Discretionary Access Protection (TCSEC criteria
C4I	Command, Control, Communications, and Computer Intelligence
CCB	Configuration Control Board
CINC	Commander in Chief
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CJTF	Commander Joint Task Force
COE	Common Operating Environment
CONOPS	Concept of Operations
DAA	Designated Approving Authority
DDA	Designated Development Activity
DDN	Defense Data Network
DIA	Defense Intelligence Agency
DICO	Data Information Coordination Office
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DJS	Director, Joint Staff
DOD	Department of Defense
DODD	Department of Defense Directive
DSAWG	DISN Security Accreditation Working Group
DSCS	Defense Satellite Communications System
DSNET1	Defense Secure Network 1
EPL	Evaluated Products List
FDDI	Fiber Distributed Data Interface
FOC	Full Operational Capability
GBS	Global Broadcast Service

GCC	Global Control Center
GCCS	Global Command and Control System
GCCS DAA	GCCS Designated Approving Authority
GCCS ISSO	GCCS Information System Security Officer
GCCS Site DAA	GCCS Site Designated Approving Authority
GCCS(T)	GCCS-TOP SECRET
GENSER	General Service
GSA	General Service Agency
GSO	GCCS Security Officer
I&A	Identification and Authentication
IDS	Intrusion Detection System
IP	Internet Protocol
IPR	Internet Protocol Router
IOC	Initial Operational Capability
ISOO	Information Security Oversight Office
ISSM	Information System Security Manager
ISSO	Information System Security Officer
ITSDN	Integrated Tactical Strategic Demonstration
Network	
J-3	Director for Operations
J-6	Director for Command, Control, Communication and Computers
JS	Joint Staff
JTF	Joint Task Force
LAN	Local Area Network
MLS	Multilevel Security
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NCA	National Command Authorities
NCSC	National Computer Security Center
NCSC-TG	NCSC-Technical Guide
NDP	National Disclosure Policy
NMCS	National Military Command System
NOC	Network Operations Center
NSA	National Security Agency
OMB	Office of Management and Budget
OPR	Office of Primary Responsibility

OT	Operational Test
PCs	Personal Computers
PMO	Program Management Office
PSN	Packet Switching Node
RA	Risk Analysis
RCC	Regional Control Center
SFUG	Security Features User's Guide
SIPRNET	Secret Internet Protocol Router Network
SMG	Standard Mail Guard
SNS	Secure Network Server
SONET	Synchronous Optical Network
SOP	Standard Operating Procedures
SSC	SIPRNET Support Center
ST&E	Security Test and Evaluation
STEP	Standard Tactical Entry Point
STD	Standard
STU-III	Secure Telephone Unit III
TCSEC	Trusted Computer System Evaluation Criteria
TFM	Trusted Facility Manual
USERID	User Identification
WAN	Wide Area Network
WSs	Workstations

Part II - Definitions

access. A specific type of interaction between a subject (i.e., a person, process or input device) and an object (i.e., an AIS resource such as a record, file, program, or output device) that results in the flow of information from one to the other. Also, the ability and opportunity to obtain knowledge of classified or sensitive but unclassified information. (DODD 5200.28)

accountability. The property that enables activities on an AIS to be traced to individuals who may then be held responsible for their actions. (DODD 5200.28)

accreditation. A formal declaration by the DAA having accreditation responsibility that the AIS is approved to operate in one or more particular security modes using a prescribed set of safeguards. Accreditation is the official management authorization for operation of an AIS and is based on the certification process and on other management considerations. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security. (DODD 5200.28)

AIS security. Measures and controls required to protect against unauthorized (accidental or intentional) disclosure, modification, or destruction of AISs and data and denial of service to process data. AIS security includes consideration of all hardware/software functions, characteristics, or features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer, and terminal facilities; management constraints; physical structures and devices; and personnel and communications controls needed to provide an acceptable level of risk for the AIS and for the data and information contained in the system. The totality of security safeguards needed to provide an acceptable protection level for an AIS and for data processed by an AIS. (DODD 5200.28)

assurance. A measure of confidence that the security features and architecture of an AIS accurately implement, mediate and enforce the security policy. If the security features of an AIS are relied upon to process sensitive information and restrict user access, the features must be tested to ensure that the security policy is enforced during AIS operation. (DODD 5200.28)

asynchronous transfer mode. An emerging technology that can transmit multi-media (digitized voice, video, and data) across local, metropolitan,

and wide area networks. ATM is an international standard defined by ANSI and ITU-TSS that implements a high speed, connection-oriented, cell switching and multiplexing technology designed to provide users with virtually unlimited bandwidth.

audit. To conduct an independent review and examination of system records and activities to test for adequacy of system controls to ensure compliance with established policy and operational procedures and recommend changes in controls, policy, or procedures. (DODD 5200.28)

audit trail. A set of records that collectively provide documentary evidence of processing used to trace from original transactions forward to related records and reports, and/or backwards from records and reports to their component source transactions.

communications security. Also, called COMSEC. The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications. Communications security includes crypto security, transmission security, emission security, and physical security of communications security materials and information.

- a. crypto security - The component of communications security which results from the provision of technically sound crypto-systems and their proper use.
- b. transmission security - The component of communications security which results from all measures designed to protect transmissions from interception and exploitation by means other than crypto analysis.
- c. emission security - The components of communications security resulting from all measures taken to deny unauthorized persons information of value possibly derived from interception and analysis of compromising emanations from crypto-equipment and telecommunications systems.
- d. physical security - The component of communications security which results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons.

computer security (COMPUSEC). Synonymous with automated information security. (NCSC-TG-004, Version 1)

configuration control. The process of controlling modifications to the system's hardware, firmware, software, and documentation that provides sufficient assurance that the system is protected against the introduction of improper modifications prior to, during, and after system implementation. Compare configuration management. (NCSC-TG-004, Version 1)

configuration management. The management of security features and assurances through control of changes made to a system's hardware, software, firmware, documentation, test, test fixtures and test documentation throughout the development and operational life of the system. Compare configuration control. (NCSC-TG-004, Version 1)

cots software. Software acquired by government contract through a commercial vendor. This software is a standard product, not developed by a vendor for a particular government project (COTS-commercial off the shelf).

countermeasure. Any action, device, procedure, technique, or other measure that reduces the vulnerability of, or threat to, a system. (NCSC-TG-004, Version 1)

data. A representation of facts, concepts, information, or instructions suitable for communication, interpretation, or processing by humans or by an AIS. (DODD 5200.28)

data integrity. The state that exists when data is unchanged from its source and accidentally or maliciously has not been modified, altered, or destroyed. (DODD 5200.28)

data owner. The authority, individual, or organization who has original responsibility for the data by statute, Executive Order, or Directive. (DODD 5200.28)

declassification. The determination in the interests of national security, classified information no longer requires any degree of protection against unauthorized disclosure, coupled with removal or cancellation of the classification designation.

declassification (of ADP Magnetic Storage Media). A procedure which will totally remove all the classified or sensitive information stored on magnetic media followed by a review of the procedure performed. A decision can then be made for (or against) actual removal of the classification level of the media. Declassification allows release of the media from the controlled environment if approved by the appropriate

authorities.

Defense Information Infrastructure (DII). The capability within DOD for local and worldwide system inter-connectivity, integration, and interoperability for the various systems that support the DOD missions and functions.

degauss. Destroy information contained in magnetic media by subjecting that media to high intensity alternating magnetic fields, following which, the magnetic fields slowly decrease.

denial of service. Action or actions that result in the inability of an AIS or any essential part to perform its designated mission, either by loss or degradation of operational capability. (DODD 5200.28)

designated approving authority (DAA). The official who has the authority to decide on accepting the security safeguards prescribed for an AIS or the official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards. The DAA must be at an organizational level, have authority to evaluate the overall mission requirements of the AIS, and to provide definitive directions to AIS developers or owners relative to the risk in the security posture of the AIS. (DODD 5200.28)

designated development activity (DDA). The activity assigned responsibility by the Joint Staff, J-6, for development of a GCCS standard software capability.

discretionary access control (DAC). A means of restricting access to objects based on the identity and need-to-know of the user, process and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject. Compare mandatory access control. (NCSC-TG-004, Version 1)

downgrade. To determine that classified information requires, in the interests of national security, a lower degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such lower degree.

downgrading (of magnetic storage media). A procedure used under the system high (e.g., TOP SECRET) mode of operation, which will reclassify the magnetic storage media to reflect the true (actual) classification of classified or sensitive information stored.

emanations security. The protection that results from all measures designed to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations.

evaluated products list (EPL). A documented inventory of equipment, hardware, software, and/or firmware that has been evaluated against the evaluation criteria found in DOD 5200.28-STD. (DODD 5200.28)

FDDI. Fiber Distributed Data Interface. An ANSI-defined standard specifying a 100-Mbps token-passing network using fiber-optic cable. Uses a dual-ring architecture to provide redundancy.

firmware. Software that is permanently stored in a hardware device that allows reading of the software but not writing or modifying. The most common device for firmware is ROM.

gateway. A device or system that enables the passage of data between networks.

GCCS network operations center (NOC). An operating center that operates 24 hours a day within the Pentagon and constantly monitors network status and coordinates network operations. This network coordination center supports the activities of the NMCC, GSO, and GCCS users.

Global Broadcast Service. A new high speed multimedia satellite communication technology.

group USERID. A USERID shared by more than one authorized user. Also implies sharing of the associated SECRET password.

individual accountability. The ability to associate positively the identity of a user with the time, method, and degree of access to a system. (NCSC-TG-004, Version 1)

information systems security. A composite of the means of protecting telecommunications systems and automated information systems and the information they process.

integrity, AIS. The capability of an AIS to perform its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. Inherent quality of protection that ensures and maintains the security of entities of an AIS.

local area network. A short-haul data communications system that

connects AIS devices in a command or base structure, including (but not limited to) workstations, front-end processors, controllers, switches, and gateways.

multilevel security. Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances but prevents users from obtaining access to information for which they lack authorization.

need to know. A determination made in the interest of U.S. national security by the custodian of classified or sensitive unclassified information, which a prospective recipient has a requirement for access to, knowledge of, or possession of the information to perform official tasks or services. (DODD 5200.28)

network. A network is composed of a communications medium and all components attached to that medium whose responsibility is the transference of information. Such components may include AISs, packet switches, telecommunications controllers, key distribution centers, and technical control devices. (DODD 5200.28)

object. A passive entity that contains or receives information. Access to an object potentially implies access to the information it contains. Object examples are records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, network nodes. (NCSC-TG-004, Version 1)

object reuse. The reassignment and reuse of a storage medium (e.g., page frame, disk sector, magnetic tape) that once contained one or more objects. To be securely reused and assigned to a new subject, storage media must contain no residual data (magnetic remanence) from the object(s) previously contained in the media. (NCSC-TG-004, Version 1)

open security environment. An environment that includes those systems in which at least one of the following conditions holds true: (a) Application developers (including maintainers) do not have sufficient clearance or authorization to provide an acceptable presumption that they have not introduced malicious logic. (b) Configuration control does not provide sufficient assurance that applications are protected against introduction of malicious logic prior to and during the operation of system applications. (NCSC-TG-004, Version 1)

operating system. An integrated collection of service routines for supervising the sequencing and processing of programs by a computer.

Operating systems control the allocation of resources to users and their programs and play a central role in assuring the secure operation of a computer system. Operating systems may perform input or output accounting, resource allocation, storage assignment tasks, and other system related functions (synonymous with monitor, executive, control program, and supervisor).

operational performance data (network). A measure of the effectiveness of the SIPRNET as seen by a user in relationship to the accomplishment of his job. Typically expressed in terms of success rate (with regard to job completion; e.g., transferring a file or accessing an application in a server or client), speed of service (system responsiveness or time required to complete a job), and accuracy.

output-only devices. Devices, such as printers, connected to a server or client (directly or through communications devices) that perform no input functions to the server or client.

overwrite. A procedure to remove or destroy data recorded on magnetic storage media by writing patterns of data over or on top of the data stored on the media.

password. A protected/private character string used to authenticate an identity. (NCSC-TG-004, Version 1)

periods processing. A manner of operating an AIS in which the security mode of operation and/or maximum classification of data processed by the AIS is established for an interval of time or period and then changed for the following interval of time. A period extends from any secure initialization of the AIS to the completion of any purging of sensitive data processed by the AIS during the period. (DODD 5200.28)

public domain software. Software acquired from government or non-government sources, often at no charge, when the source takes no responsibility for the integrity or maintenance of the software.

purge. Removal of sensitive data from an AIS at the end of a period of processing, including from AIS storage devices and other peripheral devices with storage capacity, in such a way that there is assurance proportional to the sensitivity of the data that the data may not be reconstructed. An AIS must be disconnected from any external network before a purge. (DODD 5200.28)

read access. Permission to read information. (NCSC-TG-004, Version 1)

read-only memory (ROM). A storage area in which the contents can be read but not altered during normal computer processing.

recovery procedures. The actions necessary to restore a systems computational capability and data files after a system failure.

regrade. Determining if certain classified information requires, in the interest of national defense, a higher or a lower degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such higher or lower degree. (Joint Pub 1-02)

residue. Data left in storage after processing operations are complete, but before degaussing or rewriting has taken place. (NCSC-TG-004, Version 1)

risk. A combination of the likelihood that a threat shall occur, the likelihood that a threat occurrence shall result in an adverse impact, and the severity of the resulting adverse impact. (DODD 5200.28)

risk analysis. An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of occurrence. (DODD 5200.28)

risk analysis. The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards. Risk analysis is a part of risk management. Synonymous with risk assessment. (NCSC-TG-004, Version 1)

risk management. The total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost-benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review. (NCSC-TG-004, Version 1)

root access. A function or state in which a user or program has unrestricted access to the operating system, applications programs, or data, whether in memory or on media.

sanitize. To erase or overwrite classified data stored on magnetic media for the purpose of declassifying the media.

Secret Internet protocol router network (SIPRNET). The SIPRNET is a subset of the DII and provides end to end information transfer and value added services, for the transport of data up to the SECRET level. The

SIPRNET architecture supports national defense C4I worldwide information transfer requirements. It is a router based wide area network of the DISN. It consists of routers, hubs, communications servers, multiplexers, encryption devices, switches, three RCCs, one GCC, and one SSC.

security incident. An incident involving classified information in which there is a deviation from the requirements of governing security regulations (e.g., compromise, inadvertent disclosure, need-to-know violation, and administrative deviation).

security mode. A mode of operation in which the DAA accredits an AIS to operate. Inherent with each of the four security modes (dedicated, system high, multilevel, partitioned) are restrictions on the user clearance levels, formal access requirements, need-to-know requirements, and the range of sensitive information permitted on the AIS. (DODD 5200.28)

security-relevant event. Any event that attempts to violate the security policy of the system (e.g., too many attempts to logon).

security test and evaluation (ST&E). An examination and analysis of the security safeguards of a system as they have been applied in an operational environment to determine the security posture of the system. (NCSC-TG-004, Version 1)

synchronous optical network (SONET). An emerging network that will eventually allow ATM to be deployed at rates of 622 megabytes per second, 1.2 gigabytes per second, and 2.4 gigabytes per second.

system access. Refers to access privileges given to maintainers of the operating system files or, more frequently, the generic term for users' capability to logon to a computer system or network.

system high security mode. A mode of operation wherein all users having access to the AIS possess a security clearance or authorization, but not necessarily a need to know, for all data processed by the AIS. If the AIS processes special access information, all users must have formal access approval. (DODD 5200.28)

system users. Those individuals with direct connections to the system and also those individuals without direct connections who receive output or generate input that is not reliably reviewed for classification by a

responsible individual. The clearance of system users is used in the calculation of risk index.

TEMPEST. The study and control of spurious electronic signals emitted by electrical equipment. (NCSC-TG-004, Version 1)

threat. Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service. (NCSC-TG-004, Version 1)

Trusted Computer System Evaluation Criteria (TCSEC). A document published by the National Computer Security Center containing a uniform set of basic requirements and evaluation classes for assessing degrees of assurance in the effectiveness of hardware and software security controls built into systems. These criteria are intended for use in the design and evaluation of systems that will process or store sensitive or classified data. This document is DOD 5200.28-STD and is alternately referred to as the Criteria or The Orange Book.

type accreditation. Official authentication by the DAA to employ a system in a specified environment. This authorization includes a statement of residual risk, delineates operating environment, and specific use. It is performed when multiple copies of a system are to be fielded.

user. A person who interacts directly with client/server system. In GCCS, a person or organization who has access to GCCS through a client or who is allowed to submit input to the system through other media; e.g., tape or floppy disk, and has been assigned an individual or group USERID and password. (Does not include those persons or organizations defined as customers.)

vulnerability. A weakness in system security procedures, system design, implementation, internal controls, etc., that could be exploited to violate system security policy. (NCSC-TG-004, Version 1) Vulnerability is also the susceptibility of a particular system to a specific attack, along with the opportunity available to a hostile entity to mount that attack. A vulnerability is always demonstrable, but may exist independently of a known threat. In general, a description of a vulnerability takes account of those factors under friendly control.

Appendix D
TEST AND EVALUATION GUIDANCE AND
DIRECTIVES

The v3.0 TEMP and subsequent TEMP annexes to EIPs for increments must contain the content prescribed by "DoD Regulation 5000.2-R, Appendix III, Test and Evaluation Master Plan Mandatory Procedures and Format."

For increments subsequent to the v3.0 GCCS, the content can be tailored and streamlined according to the level of potential mission consequence. Both the proposed level of testing and the assessment of the potential mission consequences justification should be presented in the tailored TEMP Annex to the incremental EIP for DOT&E and DTSE&E approval. The assessment of the necessary level of operational testing should be performed according to the DOT&E "Guidelines for Conducting Operational Test and Evaluation for Software-Intensive System Increments" reproduced in this Appendix. Note that the term "risk" in the DOT&E Guidelines was replaced here by the phrase "potential mission consequences" because the GCCS user community objected to the traditional interpretation of the term "risk" as an inability to perform a critical function.

According to two memoranda, also reproduced in this Appendix, a GCCS increment can enter the operational testing phase only if it is free of all Priority I or Priority II software errors. Since the GCCS mission requirements can be met by many alternative means and workarounds, and because available and desired software may perform a majority of the required functions, but not all, the interpretation of Priority I or Priority II problems should be made in the context of the integrated GCCS system. Therefore, GCCS users will determine whether the GCCS software is capable of performing its intended mission, with workarounds, in a representative and integrated configuration. Thus, a Priority I or II problem with a GCCS application may or may not imply a Priority I or II deficiency of the integrated GCCS system. If there are Priority I or II deficiencies of the integrated GCCS system, then the software has to be fixed or the requirement has to be waived at the flag officer level before entering operational testing or being fielded.



OPERATIONAL TEST
AND EVALUATION

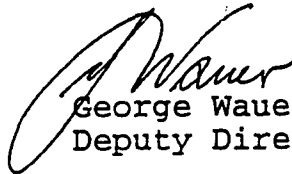
OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

11 OCT 1996

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Guidelines for Conducting Operational Test and
Evaluation for Software-Intensive System Increments

To streamline the operational test and evaluation process and to achieve "affordable confidence" for the development and procurement of software-intensive systems, the subject guideline (with all your previous substantive comments incorporated) are attached for your usage for a period of one year. At the end of the period, I plan to conduct a follow-on operational test and evaluation off-site, with your full participation, to capture lessons learned and to identify opportunities for improvements. Working together, as we have done well in the past, I believe we can complete the task of creating a flexible, responsive, and yet highly effective operational test and evaluation methodology for software-intensive systems.


George Wauer
Deputy Director

Attachment:
As stated

DISTRIBUTION:
OFFICE OF DIRECTOR, TEST, SYSTEMS ENGINEERING, AND EVALUATION
(DTSE&E), OUSD(A&T)
OFFICE OF DEPUTY UNDER SECRETARY OF THE ARMY (OPERATIONS
RESEARCH)
OFFICE OF DIRECTOR OF NAVY TEST AND EVALUATION AND TECHNOLOGY
REQUIREMENTS (N091)
OFFICE OF DIRECTOR, AIR FORCE TEST AND EVALUATION (AF/TE)
OFFICE OF COMMANDER, UNITED STATES ARMY OPERATIONAL TEST
AND EVALUATION COMMAND (OPTEC)
OFFICE OF COMMANDER, OPERATIONAL TEST AND EVALUATION
FORCE (OPTEVFOR)
OFFICE OF COMMANDER, AIR FORCE OPERATIONAL TEST AND
EVALUATION CENTER (AFOTEC)
OFFICE OF DIRECTOR, MARINE CORPS OPERATIONAL TEST AND
EVALUATION ACTIVITY (MCOTEA)
OFFICE OF DIRECTOR, DEFENSE LOGISTICS AGENCY, ATTN: CANQ
OFFICE OF DIRECTOR, JOINT INTEROPERABILITY TEST COMMAND

GUIDELINES FOR CONDUCTING OPERATIONAL TEST AND EVALUATION FOR SOFTWARE-INTENSIVE¹ SYSTEM INCREMENTS

1. BACKGROUND

An increasing number of DoD software-intensive systems are being procured with incremental acquisition strategies. The systems are deployed in a series of program increments, where each successive increment builds upon the capabilities and functionality previously deployed.

Most DoD acquisitions have traditionally employed fairly rigid testing plans in which the test phases are extensive, distinct, and dependent upon the completion of one phase prior to starting the next. The increased use of commercial-off-the-shelf (COTS) products and non-developmental items (NDI), coupled with the initiative to streamline the acquisition process, requires a more flexible and responsive operational test and evaluation strategy.

2. PURPOSE AND SCOPE

This document presents a set of guidelines for tailoring pre-deployment test events to the operational risk² of a specific system increment acquired under OSD oversight. For insignificant to moderate risk increments, these guidelines streamline the OT&E process by potentially reducing the degree of testing. These guidelines also permit the delegation of testing and fielding decisions for a specific increment to the Component.

These guidelines apply to increments of software-intensive systems acquired subsequent to deployment of the "core block,"³ which undergoes full operational testing. The OT&E of the core block will provide a performance baseline for testing subsequent increments. This revised operational testing strategy provides "affordable confidence" to the development and procurement process, while mitigating risks. Services and Agencies are encouraged to employ these guidelines for non-oversight programs as well.

3. GENERAL APPROACH

The objective of these guidelines is to provide a method for determining levels of operational testing that are appropriate to the risk posed by specific system increments. The first step is assessing risk. Risk assessments are made by the appropriate Operational Test Agency (OTA). Most are based upon two essentially independent evaluations: analysis of the factors that

¹ For the purposes of this guideline, *software-intensive* systems are computer-based information systems executing one or more resident, *separable* application software programs. Examples include automated information systems (AIS) and command and control (C2) systems. Software systems embedded in weapon systems are excluded from these procedures pending further study.

² *Risk* is a compound function of the likelihood and mission impact of an increment's failure to be operationally effective and suitable.

³ The *core block* of a system provides the basic infrastructure necessary to support the ensuing incremental functionality. This first increment also delivers the initial operational capabilities, usually a worthwhile standalone system even without additional increments. It normally consists of basic hardware, system software and tools, and fundamental applications.

affect the likelihood of success of an increment, and an understanding of the mission impact of increment failure.

The next step is to define the amount of operational testing that will provide sufficient, but not unnecessary, assurance that the risk will be mitigated to an acceptable level. The appendices to this document provide suggested techniques and recommendations for assessing risk and determining appropriate levels of testing.

The OTA then presents the proposed operational test strategy to the Director, Operational Test and Evaluation (DOT&E), during the normal test concept briefing; if it is approved, it is then implemented. If the increment poses insignificant to moderate risk, the OT&E and fielding decision may be delegated to the Component.

4. IMPLEMENTATION

A. Prepare risk assessment. The OTA, with inputs from the Program Management Office (PMO) and the user, conducts a risk assessment that includes the evaluation of potential threats to success and the mission impact of failure.

B. Determine appropriate level of OT&E. Based upon the assessed risk, the OTA proposes an appropriate level of OT&E for the new increment during the OT&E concept briefing to DOT&E. For insignificant to moderate risk increments, the operational testing, evaluation, and fielding decision may be delegated to the Component.

C. Develop OT&E plan appropriate for the validated level of test. The OTA develops an operational test and evaluation plan based upon the DOT&E-approved test concept.

D. Conduct test activities and prepare report. The OTA conducts the test and collects the data. The OTA then prepares an independent evaluation report (IER), and provides a copy to the appropriate offices of the Component and to DOT&E.

E. Provide operational effectiveness and suitability recommendations. The IER and any additional evaluation data are analyzed by DOT&E for test events conducted under OSD oversight. For non-delegated increments, DOT&E provides independent operational effectiveness and suitability recommendations to the Milestone Decision Authority (MDA). For delegated increments, the OTA provides operational effectiveness and suitability recommendations to the Component Acquisition Executive (CAE), who makes the fielding decision for the increment.

5. EFFECTIVE DATE

October 15, 1996

Enclosures:

Appendix A - Elements of Risk Assessment for System Increments

Appendix B - Determining Appropriate OT&E for System Increments

Appendix C - Responsibilities for and Schedule of OT&E Actions

APPENDIX A

ELEMENTS OF RISK ASSESSMENT FOR SYSTEM INCREMENTS

There are two primary factors in assessing the risk of a system element: the likelihood of failure and the impact on the mission of an increment's failure to be operationally effective and suitable. Fortunately, these two components need to be evaluated only to the degree required to decide among a few distinct levels of operational testing.

This appendix will discuss these two fundamental elements of risk assessment: the likelihood of failure, which will be evaluated via a surrogate method, and the mission impact of failure, which will be approached in a more direct fashion. The final step is the fusion of these two evaluations into an assessment of the overall risk of a system increment. The specific evaluation procedures presented in this appendix are provided as examples, rather than requirements.

1. Identification and Evaluation of Threats to Success for Increments

The data required to accurately define the true probability of failure of an increment are not likely to be available. As an alternative approach, the analysis can be based upon an evaluation of a comprehensive set of factors that have been identified as potential threats to the success of a software-intensive increment. These threats to success can be evaluated relative to the specific increment, and a general estimate of potential effects can be determined. The evaluation of the cumulative effect of the threats to an increment's success is analogous to determining the likelihood of failure for the increment. Of necessity, this aggregate assessment is usually a judgment call.

Most concerns associated with the deployment of a new, generic, software-intensive system increment occur in six primary categories of threats to success, although fewer or more categories may be appropriate for a specific increment. Further, the six categories may have significantly different relative sensitivities for any particular increment. The six categories of threats to success suggested are:

- Development
- Implementation
- Technology
- Complexity
- Safety
- Security.

The OTA should first assess the threat to an increment's success from each separate area, by examining the particular characteristics of the increment and its development. This evaluation is guided by the specific issues identified with each category. Clearly, not all issues within a category will have equal importance.

Then, based upon these assessments and the relative significance of each area, the OTA should make an overall evaluation of the likelihood of the increment's failure to be operationally effective and suitable. Not all categories need to be given equal importance. The evaluator

should base this judgment upon the particulars of the increment, the development process, and the utility and reliability of available data. Note that the categories and issues presented here are merely examples; the evaluator should always consider risk factors specific to the increment. In other words, *use good judgment, based on detailed knowledge of the increment.*

Each category should be evaluated as accurately as possible, and at least to the levels of resolution described below. Each of these levels is defined in terms of idealized, typical characteristics; actual assessments will be a mix of positive, neutral, and negative characteristics.

- Insignificant Threat to Success (Insignificant Likelihood of Failure) – Increments posing this level of threat to success are typically small, simple modular increments that come from a highly reliable developer and an ideal development environment. Additional characteristics that support this assessment are a program's demonstrated success with all previous increments, employment of very mature technologies, excellent training programs or highly experienced users, no impact upon other system elements, and no safety or security issues.
- Low Threat to Success (Low Likelihood of Failure) – Increments posing this level of threat to success may be small- to medium-sized, involving few complicated issues. Other characteristics justifying a low threat to success are a solid development environment with few shortcomings, employment of stable technologies, capable users, little interaction with basic system elements, and few safety or security issues.
- Moderate Threat to Success (Moderate Likelihood of Failure) – This level of threat to success is typically assigned to medium- to large-sized increments having several complex elements and employing recent technological developments. Other system characteristics supporting this level of assessment are complicated interfaces with other systems, interacts significantly with system resources, and several safety and security issues.
- High Threat to Success (High Likelihood of Failure) – This highest level of threat to success typically involves large to very large, complex, multi-functional increments. Other characteristics include untested or unreliable development environments with poor performance histories, new technologies, many untested interfaces, new or untrained users, and multiple safety and security issues.

It is unlikely that all six categories of evaluation will be assigned the same level of threat to success. One simple scheme of evaluation would be to assign to the increment as a whole a level equal to or greater than the highest level of threat to success determined for any single category. For example, if the highest level category poses a *moderate* threat to success, then the overall level should be no lower than moderate. If two or more important categories are rated as moderate, then the overall level might be elevated to a high threat to success (or high likelihood of failure).

Example Issues for Evaluating Threats to Success

The following issues represent some potential threats to an increment's success. Detailed knowledge of a particular system increment will, of course, tailor the assessment.

a. Development

- Have mission needs been adequately described and user requirements clearly identified?
- Do the requirements address operational needs rather than specifying a technical solution?
- What is the developer's Capability Maturity Model rating as defined by the Software Engineering Institute?
- How extensive was the developmental test program for this increment?
- Does the developer employ a robust set of software management indicators?
- Are interfaces with existing systems fully documented and under configuration control?
- Does the developing contractor's test agent have sufficient experience and technical expertise to conduct a proper technical evaluation?
- Has the necessary integration and regression testing been conducted?
- Were any Priority 1 or Priority 2 problems¹ experienced with the last increment from this development team?
- How numerous and how significant are the deficiencies identified in previous tests of the new increment?
- What is the history of the developer regarding similar programs?
- What is the history of the developer with respect to previous increments?
- How effective is the established configuration management process for the program development and/or installed systems?
- How extensively have prototypes been used to evaluate acceptance by typical users?
- Have exit criteria been identified for developmental testing of this increment?

b. Implementation

User:

- Is the user committed to the successful implementation of the new increment?
- Have operational and user support procedures been developed and readied for implementation along with the new increment?

¹ As defined in MIL-STD-498.

- Do the operators possess the skill levels required to use the increment's capabilities effectively?
- Has an adequate training plan been developed or implemented to include reorientation and sustainment training?

Organization:

- Is the receiving organization committed to the successful implementation of the new increment?
- Is the receiving organization prepared for the changes in business processes associated with the new increment?
- Have new standard operating policies and procedures been developed or implemented to use the capabilities of the new increment?
- Has the receiving organization developed plans for continuity of operations during the installation of the new increment?

c. Technology

- How dependent is the new increment upon new technologies (hardware and software)?
- What is the commercial tempo of change in the technology areas represented in the increment?
- How mature are the new technologies incorporated into the increment?
- Does the new increment introduce any new standards or protocols?
- Does the integration of the entire system (e.g., hardware, software, communications, facilities, management, operations, sustainment, personnel) present unusual challenges?
- Does the system include the necessary system administration capabilities?
- If the increment is primarily COTS, NDI, or GOTS (government-off-the-shelf), what is the past performance and reliability?
- For new technologies, what is the performance record in other applications?

d. Complexity

- How complex is the new increment (e.g., McCabe and Halstead metrics, or as compared to other fielded increments)?
- How many agents (government, contractors, sub-contractors) participated in the development of this increment?
- How stable are the system requirements?

- What is the proportional change to system hardware and software introduced by the new increment?
- What is the cumulative change to system hardware and software since the last full operational test?
- Is the new system (including the increment of interest) to be integrated with other systems during development or deployment?
- How complex are the external system interface changes (hardware, software, data) in the new increment?
- How complex are the user interactions with the new increment?
- How complex are the interactions of the new increment with the fielded databases?
- To what extent does the new increment introduce changes that place in jeopardy or modify the system data structures?
- Does the new increment implement a change in executive software (operating system or database management system)?

e. Safety

- Does the system present any safety hazards to the operators or operational environment?

f. Security

- Does this system require multi-level security?
- Can the new increment affect the security or vulnerability (to information warfare) of the installed system?
- If it has external interfaces, has the system been tested for unauthorized access?

In addition to the above general matters, there may be other overriding concerns — conditions that are potentially so important that, if they are present, a thorough and comprehensive operational testing effort is *mandatory*.

2. Identification and Evaluation of Mission Impact of Increment Failure

The mission impact assessment should consider the impact of the possible failure of the new increment on the mission of the whole system. Table A-1 provides a typical set of potential mission impact assessments, related to resolution of system critical operational issues (COIs).

Table A-1. Degree of Mission Impact

Effect on Mission	Definition
Minor Impact	Increment failure would cause noticeable problems, but no major interference with mission accomplishment. System COIs can be satisfactorily resolved, even without increment success.
Moderate Impact	Increment failure could cause substantial degradation of mission-related capabilities. System COIs are moderately dependent upon increment performance.
Major Impact	Element is required for mission success. System COIs are critically dependent upon increment performance.
Catastrophic Impact	The element is required for mission success, and its malfunction could cause significant damage to the installed system, to other interconnected systems, or to personnel.

The evaluator must make a mission impact assessment for each of the mission areas affected by the new increment. The total impact to the mission is then assessed as the highest impact noted for any area of concern, or at a level above the highest level noted if many lower potential impacts are evident.

3. Assessing the Risk of a System Increment

When the mission impact and likelihood of failure of an increment have been determined, the risk assessment may be made as the *product* of these two basic elements. However, in assessing risk, the mission impact should be weighted more heavily than the likelihood of failure. Appendix B presents a direct method for determining the proper level of operational testing (OT) from the levels of mission impact and likelihood of failure.

APPENDIX B

DETERMINING APPROPRIATE OT&E FOR SYSTEM INCREMENTS

The specific evaluation procedures presented in this appendix are provided as examples, rather than requirements.

1. Multiple Levels of OT&E for System Increments

The tester must determine the level of operational testing that most effectively provides "affordable confidence" that an increment will meet mission needs. A *range* of test activities should be considered and matched to the risk of the specific system increment. The range of operational testing for increments developed subsequent to the core system extends through four levels, from an abbreviated assessment to a full, conventional operational test and evaluation.

For each of these four levels of OT&E, it is presumed that user representatives have developed appropriate concepts of operations, policies, procedures, training, support, and contingency plans for a full operational deployment. Where these are lacking, the OTA must consider associated risk factors as high, increasing the level of OT required. It is also presumed that the exit criteria from developmental testing have been satisfied and that all previously deployed increments are functioning properly prior to the fielding of any new increment.

Of course, the detailed design of testing activities at each level of testing must be based upon the fundamental objective of evaluating the ability of the tested system to accomplish its mission goals when deployed. The increment's mission goals are expressed in the measures of effectiveness and suitability and the COIs stated in the Test and Evaluation Master Plan (TEMP).

Level I: Abbreviated Assessment – After complete and successful developmental testing, permit *limited* fielding and assess feedback from the field (by the OTA) prior to full fielding. Contractor presence is permitted during the Level I test. PMO-prepared and OTA-validated plans for recovery from failures *must* be in place prior to limited fielding.

Level I testing is appropriate for maintenance upgrades and increments that provide only minor system enhancements, pose an insignificant risk, and can be easily and quickly removed. Increments judged to be of sufficiently low risk for Level I testing will usually be delegated to the Component for testing, evaluation, and fielding decisions. The OTA prepares an assessment report to support any fielding decision. A copy of the assessment report is to be provided to the DOT&E. Key features of the Abbreviated Assessment are:

- It is essentially a developmental testing (DT) effort.
- The OTA monitors selected developmental/technical testing activities.
- Limited fielding is permitted prior to the OTA evaluation.
- The OTA prepares an assessment report for the CAE to support a fielding decision by the Milestone Decision Authority. For non-delegated increments, DOT&E will prepare an independent evaluation of the operational

effectiveness and suitability for the OSD MDA regarding the fielding decision.

Level II: Alpha Test¹ – Assessment performed by an OTA primarily using DT data and independent “over-the-shoulder” observations. The OTA may prescribe and observe operationally realistic test scenarios in conjunction with DT activities. Contractor presence is permitted during the Alpha Test. DOT&E may, of course, observe any OT activity.

Level II testing should be applied to increments that provide only minor system improvements and present a minor risk. Such lower risk increments have only minimal potential to impact other system applications, and *cannot* disrupt the basic system's ability to support the mission. After thorough Alpha testing, an increment may be deployed to selected operational sites for additional feedback (collected by the OTA) if needed prior to full fielding. Features of the Alpha Test are:

- It is essentially a combined DT/OT testing effort.
- The assessment is based primarily upon close monitoring of selected developmental/technical activities, and upon DT results.
- Prior to the limited fielding, plans must be in place for recovery from failures.
- The OTA evaluates the limited fielding results and reports on the operational effectiveness and suitability to the CAE to support a fielding decision by the MDA.
- A copy of the evaluation report is provided to DOT&E.
- For non-delegated increments, DOT&E will prepare an independent evaluation of the operational effectiveness and suitability for the OSD MDA regarding the fielding decision.

Level III: Beta Test¹ – OTA personnel coordinate the Beta Test, carried out by user personnel in an operational environment, and evaluate the operational effectiveness and suitability primarily using OT data collected independently. The Beta Test is conducted at one or more operational sites. In addition to normal user operations, the OTA may prescribe that scripted test events be executed and observed. Level III testing may be conducted in two phases. The Program Management Office controls Phase I, allowing contractors to fine tune the system, but the OTA supervises Phase II, which defines an operational period without PMO or contractor participation. OT evaluators, of course, are allowed during both phases.

The Beta Test is suitable for increments supporting modest, self-contained, system improvements that present a moderate level of risk, but are limited in the potential disruption to an installed system. Features of Beta Testing are:

¹ The terms *Alpha Test* and *Beta Test*, as used here, share the same basic principles as in commercial practice, but have been adapted to the DoD acquisition environment.

- Actual operators are at the operational site(s) performing real tasks.
- The emphasis is on assessment and evaluation.
- It is less formal than a full operational test.
- Prior to fielding, plans are in place for recovery in the event of failure.
- The OTA prepares an evaluation of operational effectiveness and suitability for the CAE. For non-delegated increments, DOT&E will prepare an independent evaluation of the operational effectiveness and suitability for the OSD MDA regarding the fielding decision.
- A copy of the evaluation report is provided to DOT&E.

Level IV: Full Operational Test – Determine the operational effectiveness and suitability of a new increment by evaluating affected COIs under full OT constraints. This is the highest level of operational test and the most comprehensive. The OTA carries out test events in an operational environment. The OTA evaluates and reports on the operational effectiveness and suitability of a new system increment based upon all available data, especially OT data that was independently collected. Representatives of DOT&E monitor the test events for the OSD oversight programs. In special cases, the verification of minor capabilities and secondary issues may be relegated to lower levels of testing. Level IV testing must comply with all provisions of the DoD 5000 series regulations.

2. Matching OT&E to Risk Assessment

The OT&E Action Determination Matrix shown in Table B-1 forms the basis for relating the assessed failure potential (threat to success) and mission impact to an appropriate level of OT&E. The matrix provides for the four levels of OT&E described in the last section.

Table B-1. OT&E Action Determination Matrix

Failure Potential	Effect on Mission			
	Minor Impact	Moderate Impact	Major Impact	Catastrophic Impact
Insignificant	I	I-II	II-III	III-IV
Low	I-II	II-III	III-IV	IV
Moderate	II-III	III-IV	III-IV	IV
High	III-IV	III-IV	IV	IV

APPENDIX C

RESPONSIBILITIES FOR AND SCHEDULE OF OT&E ACTIONS

1. Responsibilities

- a. Operational Test Agency – With regard to the OT&E for a follow-on system increment, the OTA is responsible for:
 - Determining the type of data and level of detail required for assessing the threats to increment success.
 - Collecting and analyzing information concerning potential threats to the success of the system increment, and determining the likelihood of failure based upon those threats.
 - Determining the type of data and level of detail required for assessing the potential mission impact of the failure of a system increment.
 - Collecting, analyzing, and determining the potential mission impacts associated with the system increment.
 - Determining an appropriate level of OT&E according to the risk assessment.
 - Developing and presenting a test concept briefing to the DOT&E.
 - Developing and coordinating the applicable level of operational test plans.
 - Validating recovery plans prior to deployment of an increment to any operational test sites.
 - Conducting the approved level of OT&E.
 - Developing the applicable independent evaluation report and providing it to the appropriate organizations.
 - Making operational effectiveness and suitability recommendations.
- b. Program Management Office – The PMO is responsible for:
 - Providing the programmatic data required to evaluate threats to the success of the new increment to the OTA action officer and user representative.
 - Providing the technical information requested to support the evaluation of each significant threat to the increment's success.
 - Developing recovery plans prior to fielding of an increment to any operational test sites.
 - Certifying the increment's readiness for OT&E.

c. User – The user (or user representative) is responsible for:

- Participating in the planning and execution of the OT&E.
- Providing the OTA with information regarding mission impacts of increment failure.
- Assisting the PMO in developing recovery plans, including workarounds for possible increment malfunctions.

d. Director, Operational Test and Evaluation (DOT&E) – In addition to the statutory and regulatory OT responsibilities of the DOT&E,² the office of the DOT&E is responsible for:

- Providing guidance as needed in the preparation of risk assessments, and determining the appropriate level of OT.
- Evaluating and responding to the operational test concept, and approving if appropriate.
- Evaluating and responding to the operational test plan, and approving if appropriate.

2. SCHEDULE OF ACTIVITIES

Table C-1 shows key OT activities, schedules, and responsibilities.

² As described in USC, Title X. DoDD 5000.1, DoD 5000.2-R, and other applicable documents.

Table C-1. Operational Testing Actions, Schedules, and Responsibilities

Action	When	Responsible Agency	Approval Agent	Comments
Prepare Program Risk Assessment	As soon as data becomes available	OTA	Component	OTA and PM conduct assessments with information provided by PM and with participation of user and other appropriate Component agencies
Determine Level of Operational Test	Upon completion of risk assessment	OTA	Component	Based on risk assessments
Develop Test Concept and Outline Operational Test Plan	Upon decision regarding level of OT	OTA	Component	Brief elements within Component, as required.
Present Test Concept Briefing to DOT&E	At least 120 days prior to start of OT	OTA	DOT&E	If approved by DOT&E, proceed to next step. Otherwise, revise test concept and brief again.
Complete Operational Test Plan ³	Submit to DOT&E at least 60 days prior to start of OT	OTA	Component, DOT&E	Brief elements within Component, as required.
Conduct Operational Test		OTA	Component	DOT&E may observe. Data supplied to DOT&E for non-delegated increments.
Analyze Test Results and Prepare Report	Complete within 90 days of test completion	OTA	Component	OTA briefs DOT&E and PM, plus other Component elements as required, on test results. DOT&E prepares independent evaluation for non-delegated increments.
Prepare and Present Deployment Recommendations to MDA		1) OTA 2) DOT&E	MDA	OTA provides recommendations to the Component MDA for delegated increments. DOT&E provides recommendations to the OSD MDA for non-delegated increments.

³ Following this stage, the PM or Program Executive Officer will need to certify that the increment is ready for operational testers to begin evaluation at the appropriate level.



OFFICE OF THE SECRETARY OF DEFENSE
WASHINGTON, DC 20301-1700

31 MAY 1994

FINAL TEST
EVALUATION

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS

ATTENTION: SERVICE ACQUISITION EXECUTIVES
ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL,
COMMUNICATIONS & INTELLIGENCE)
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
DIRECTOR, DEFENSE LOGISTICS AGENCY
DIRECTOR FOR FORCE STRUCTURE, RESOURCES &
ASSESSMENT, JOINT STAFF (J-8)
DIRECTOR, TEST AND EVALUATION, OUSD(A&T)
DEPUTY UNDER SECRETARY OF THE ARMY (OPERATIONS
RESEARCH)
DIRECTOR, NAVY TEST & EVALUATION & TECHNOLOGY
REQUIREMENTS
DIRECTOR, AIR FORCE TEST & EVALUATION

SUBJECT: Software Maturity Criteria for Dedicated Operational
Test and Evaluation of Software-Intensive Systems

Reference: GAO/NSIAD-93-198, "Test and Evaluation: DoD Has Been
Slow in Improving Testing of Software-Intensive
Systems," dated September 29, 1993

As a part of the Department's initiative to address the
General Accounting Office's (GAO) recommendations on the
Department's test and evaluation policy of software-intensive
systems, I am issuing the following guidance to establish the
software maturity criteria for the dedicated OT&E (in support of
full rate production decisions or deployment decisions) of
software-intensive systems. It is my intent to include this
guidance in the revisions to the DoD 5000 and 8120 policy
documents.

To improve the success rate of OT&E for software-intensive
systems, and to prevent immature software-intensive systems from
entering OT&E, software maturity must be demonstrated prior to the
start of the dedicated OT&E. The following conditions must be
satisfied and the results presented at the operational test
readiness review that precedes the OT&E:

a. The system must not possess any known Priority I or
II problems (as defined by the DoD-STD-2167A) that impact the OT&E
so as to constitute a deficiency relative to a critical
operational issue. Priority III problems must be documented with
appropriate impact analyses completed. These impact analyses must
focus on the problems' potential impact to the system's mission
capability and the ability to resolve the affected critical
operational issues. After the problems and their associated

impact analyses are reviewed by the functional proponent, operational test agency, and other participating organizations, recommendations on whether to proceed, delay, or cancel the OT&E can be made to the designated Service or Agency operational test certification official.

b. System functionality to be operationally tested and evaluated must be available prior to the start of OT&E and must have been developmentally tested. In particular, the system features that are required to support specific requirements and the system interfaces that are required to inter-operate with external systems must be certified to be functional, preferably in an operationally realistic environment (real users, data, procedures, etc.) against operational requirements.

c. The program management office in conjunction with the Service's or Agency's independent evaluator must identify all the unmet critical technical parameters and open deficiencies that have been noted during the developmental test and evaluation. During certification of readiness for dedicated OT&E, the acquisition executive must certify and the operational test agency must agree that the software requirements and design are stable, that software and interface testing of sufficient depth and breadth has been performed, and that required functionality has been successfully demonstrated at the system level in developmental testing. Impact analyses, on the shortfalls' potential impact to the system's mission capability and the ability to resolve the affected critical operational issues, must be completed.

d. A deficiency identification, tracking, and reporting system must be in place to support the monitoring of deficiency reports by the operational test agency. Further, a software configuration management system with the associated control procedures must be in place prior to the start of OT&E. Software-intensive systems to be operationally tested must be baselined in the configuration management system. During the operational test phase, the operational test agency must have complete access to the configuration management system.

e. Software or firmware changes, if any, must be completed prior to the start of OT&E and must not be implemented during the OT&E unless specifically acknowledged and concurred by the responsible operational test agency. The expected impact of these changes on the OT&E data stream and the evaluation of the critical operational issues must be addressed by the responsible operational test agency to assist in the decision to allow the change(s) during OT&E.


Director



ION AND
OLOGY

OFFICE OF THE UNDER SECRETARY OF DEFENSE

3000 DEFENSE PENTAGON
WASHINGTON DC 20301-3000



23 MAY 1994

MEMORANDUM FOR DISTRIBUTION

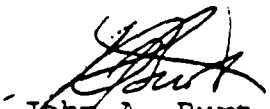
SUBJECT: Development Test and Evaluation (DT&E) Policy Guidance
for Software-Intensive Systems in Support of
Recommendations from the General Accounting Office
(GAO)

The GAO report GAO/NSIAD-93-198, "Test and Evaluation: DoD
Has Been Slow in Improving Testing of Software-Intensive
Systems," dated September 29, 1993, made four recommendations:

- 1) Establish testing requirements for software
maturity, regression testing, and temporary software fixes;
- 2) The results of Developmental Test and Evaluation
must demonstrate an appropriate level of software maturity prior
to the start of Operational test and evaluation;
- 3) Define software related exit criteria for certifying
a system's readiness for operational testing at Milestone II; and
- 4) A common core set of management metrics are to be
developed and approved at Milestone II.

The attached Guidance for GAO recommendations 1,3, and 4 is
intended to implement the three recommendations addressed by
OUSD(A&T) T&E. This guidance will be implemented in revisions to
the DoD 5000 and 8120 policy documents. The Director,
Operational Test and Evaluation will provide guidance for GAO
recommendation 2.

The attached guidance incorporates the comments received
from the DoD Components on the Draft Guidance attached to the
OUSD (A&T) memorandum, subject: "Developmental Test and
Evaluation (DT&E) Criteria for Software-Intensive Systems, dated
April 4, 1994. The guidance is meant to augment, but not
replace, the existing Service and Agency guidance on software
testing in order to improve the effectiveness of DT&E.


John A. Burt
Director
Test and Evaluation
OUSD (A&T)

Attachment

Distribution:

JOINT STAFF, DIRECTOR FOR FORCE STRUCTURE, RESOURCES AND
ASSESSMENT (J-8)
ASSISTANT SECRETARY OF DEFENSE FOR COMMAND, CONTROL,
COMMUNICATIONS AND INTELLIGENCE
DEPUTY UNDER SECRETARY OF THE ARMY (OPERATIONS RESEARCH)
DIRECTOR, TEST AND EVALUATION, HEADQUARTERS USAF
DIRECTOR, NAVY TEST AND EVALUATION
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
DIRECTOR, DEFENSE LOGISTICS AGENCY
DIRECTOR, DEFENSE MAPPING AGENCY
DSMC
DOTE

**DoD Test and Evaluation Policy Guidance
for Software-Intensive Systems**

Implementation of GAO Recommendation 1: Testing requirements are established for software maturity, regression testing and the use of temporary software fixes during testing.

a. The program management office for a software-intensive system shall propose a maturity metric, for use in monitoring and managing the program throughout the Development Phase, and shall submit the metric for approval by the appropriate acquisition authority. The quality metrics listed by the Army's Software Test and Evaluation Panel (STEP) may be used as a basis for obtaining the maturity metric.

b. All DoD Components shall, prior to any government system-level developmental testing, establish and freeze the software configuration. Any changes proposed during system-level testing, to include software fixes, shall be kept to a minimum and shall be reviewed and approved by the Component's configuration control board for the respective acquisition program using MIL-STD-973 as guidance. All software development shall be fully documented.

c. Sufficient regression testing shall be conducted for all software changes, throughout the development cycle and after implementation of configuration control, to ensure that changes designed to correct specific problems do not result in additional defects. The scope of regression testing is determined by the developer/contractor prior to freezing the configuration, and determined by the test organization, developer and independent evaluator after the configuration is frozen. Changes made to the software, during system-level testing or later, can impact the resources and schedule of a Component's test organization and therefore impact the testing of other programs. All software configuration changes shall be documented using MIL-STD-973 as guidance.

d. The DoD Component shall ensure that the proper levels of testing have been accomplished and determine if additional testing is required before certification for independent operational tests.

Implementation of GAO Recommendation 3: Program management officials shall define software related exit criteria for certifying a system's readiness for Operational Testing at Milestone II.

Department of Defense Instruction 5000.8, Part 8, requires certification that the system is ready for the dedicated phase of operational test and evaluation to be conducted by the DoD Component operational test activity. In order to

comply with this policy,

a. Each DoD Component shall develop a process, or modify an existing process, for program management officials to define software related exit criteria at Milestone II for software-intensive systems for the purpose of certifying the system's readiness for operational testing.

b. These exit criteria are required to be defined at Milestone II. These criteria may be modified and/or criteria may be added as appropriate during the system's development phase.

3. Implementation of GAO Recommendation 4: A common core set of management metrics for software shall be developed by the services for major defense programs early in the development cycle to be approved at Milestone II.

The following core set of management metrics shall be implemented by DoD Components for major software-intensive defense programs. These metrics comprise a minimum set for information gathering over the life cycle of a program, and must be developed to support program approval at Milestone II. Each DoD Component may develop and implement additional metrics for Milestone II or for subsequent portions of the life cycle to aid in program monitoring or to support other needs of the DoD Component. One metric that should be selected at Milestone II for use during the development phase is "fault profile," which is comprised of the total number of faults over time (identified and corrected) and the severity of these faults categorized as Priority 1, 2, 3 and 4 versus set periods of time that the faults are open (e.g., 0-15 days, 15-30 days, 30-60 days, etc.). Additional metrics are:

a. Cost. A cost metric shall be developed which will provide insight into how well the cost of software development is controlled. The cost metric should address software development costs as well as the life-cycle cost impacts of the software development;

b. Schedule. A schedule metric shall be developed which will indicate changes and adherence to the planned schedules for major system development milestones, activities and key software deliverables; and

c. Requirements Traceability. A requirements traceability metric shall be developed which will measure the adherence of the software products (including design and code) to their requirements at the system level.

REPORT DOCUMENTATION PAGE*Form Approved*
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (Leave blank)**2. REPORT DATE**
September 1997**3. REPORT TYPE AND DATES COVERED**
Final**4. TITLE AND SUBTITLE**

An Evolutionary Acquisition Strategy for the Global Command and Control Systems (GCCS)

5. FUNDING NUMBERSC-DASW01-94-C-0054
TA- T-J6-1492**6. AUTHOR(S)**

Richard H. White, David R. Graham, Johnathan Wallis

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)Institute for Defense Analyses
1801 N. Beauregard Street
Alexandria, VA 22311**8. PERFORMING ORGANIZATION
REPORT NUMBER**

IDA Paper P-3315

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)Assistant Secretary of Defense (Command, Control, Communications, and
Intelligence)
The Pentagon
Washington, DC 20301**10. SPONSORING/MONITORING
AGENCY REPORT NUMBER****11. SUPPLEMENTARY NOTES****12a. DISTRIBUTION/AVAILABILITY STATEMENT**

Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE**13. ABSTRACT (Maximum 200 words)**

This paper sets forth an evolutionary acquisition strategy for the Global Command and Control System. The strategy is the product of the GCCS Integrating, Integrated Product Team, and is fully compliant with DoD Regulation 5000.2-R. The concept of an Evolutionary Phase Implementation Plan (EPIP) is introduced, and the relationships between the strategy and traditional acquisition procedures are made.

14. SUBJECT TERMS

Evolutionary Acquisition, Evolutionary Phase Implementation Plan, EPIP, Acquisition Reform, MAISRC

15. NUMBER OF PAGES

226

16. PRICE CODE**17. SECURITY
CLASSIFICATION
OF REPORT**

UNCLASSIFIED

**18. SECURITY
CLASSIFICATION
OF THIS PAGE**

UNCLASSIFIED

**19. SECURITY
CLASSIFICATION
OF ABSTRACT**

UNCLASSIFIED

**20. LIMITATION OF
ABSTRACT**

UL